CZASOPISMO BEZPŁATNE
ISSN: 1505-2419 DWUMIESIĘCZNIK NR 1(131)/2020

ZABEZPIECZENIA

POLON-ALFA

PROJEKTUJEMY *zgodnie ze sztuką*

SYSTEMY SYGNALIZACJI POŻAROWEJ

- innowacyjnie rozproszony **POLON 6000**
- interaktywny **POLON 4000**
- konwencjonalny **IGNIS 1000/2000**

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

SYSTEM DETEKCJI GAZÓW SDG 6000

POLON-ALFA S.A.
85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl

next!

Jesteśmy z Wami już od 18 lat!

2002
pierwsze wdrożenie KRONOS
programu do monitoringu (SSWiN i PPOŻ)

2003
integracja **urządzeń telemetrycznych**
(pomiary analogowe)

2004
pierwsza na rynku w pełni **sieciowa wersja**
KronosNET w architekturze trójwarstwowej

2005
integracja **wideo** (CCTV)
pierwsze **konsole mobilne**

2006
integracja **telefonów**
kontrola wartowników

2007
obsługa pojazdów (GPS)
rozpoczęcie **sprzedaży za granicą**

2008
premiera **KronosNET 2.0** pakietu do zarządzania
agencją ochrony (moduły serwisu i rozliczeń)
uzyskanie certyfikatu ISO 9001:2000

2009
pierwsze **konsole webowe**

2010
Złoty Medal MTP

2012
rozpoczęcie **produkcji urządzeń**
(Xamelo i później Arrow)

2013
premiera **Kairos** - systemu do zarządzania
bezpieczeństwem budynków

2016
premiera **KronosNET 3.0**

2018
premiera **KronosNET 4.0**

2019
Kronos Alicja
automatyczny dyspozytor
oparty o sieci neuronowe

Chcesz wiedzieć co będzie dalej?
Śledź nas na Facebooku!

tel.: +48 33 810 56 45 · e-mail: office@next.biz.pl · www.next.biz.pl

SPIS TREŚCI

Nowości produktowe

Wydarzenia, informacje

Temat numeru
nowe produkty i rozwiązania w systemach kontroli dostępu

Normalizacja

Inteligentny budynek

Nowe technologie

Ochrona fizyczna

Zintegrowane systemy dozorowe
firm Videotec i Sony

Firma **Videotec** informuje, że w głowicach kamerowych PTZ z nowej serii **ULISSE EVO** zastosowane będą moduły kamerowe **Sony FCB-EV7520** odznaczające się bardzo wysoką czułością. Głowice ULISSE EVO będą wyznaczały nowy poziom jakościowy w dziedzinie urządzeń służących do nadzoru portów lotniczych, obiektów infrastruktury krytycznej i ruchu drogowego.

Moduł kamerowy Sony FCB-EV7520 użyty w głowicy ULISSE EVO ma obiektyw z trzydziestokrotną regulacją ogniskowej oraz przetwornik CMOS Exmor RTM o rozmiarach 1/2,8". Moduł wytwarza obraz o rozdzielczości Full HD z prędkością 60 klatek na sekundę.

W module kamerowym wykorzystywany jest usprawniony algorytm stabilizacji obrazu, który umożliwia wykrywanie nawet najmniejszych drgań głowicy. Dzięki temu wszelkie rozmycia obrazu są dynamicznie korygowane. Jest to przydatne w systemach kontroli ruchu drogowego, w których głowica może być targana przez wiatr lub narażona na wibracje mechaniczne, szczególnie jeśli jest zainstalowana na konstrukcji podatnej na wstrząsy, takiej jak most lub słup.

W głowicy ULISSE EVO z modułem kamerowym Sony można ustawić do 24 dynamicznych masek prywatności. Maski te zmieniają swoje rozmiary i kształt w zależności od ustawienia azymutu i po-

chylenia głowicy, a także w zależności od zmian ogniskowej obiektywu, dzięki czemu obiekty, które nie powinny być widoczne, pozostają ukryte.

Najnowsze moduły kamerowe firmy Sony mają funkcje rozszerzania zakresu dynamiki i kompensacji nadmiernego oświetlenia obserwowanej sceny, które zapewniają optymalizację odwzorowania zarówno bardzo jasnych, jak i bardzo ciemnych fragmentów obrazu. Wysoka czułość tych modułów umożliwia wytwarzanie kolorowych obrazów przy oświetleniu sceny przekraczającym 0,0013 lx, a obrazów czarno-białych przy oświetleniu przekraczającym 0,0008 lx.

Jako wyposażenie dodatkowe oferowane są oświetlacze pracujące w podczerwieni, dzięki którym można korzystać z głowic ULISSE EVO w zupełnych ciemnościach. Funkcja *defog* zapewnia wytwarzanie czytelnego obrazu nawet w przypadku zamglenia lub zadymienia.

Użyty w głowicy ULISSE EVO moduł kamerowy Sony FCB-EV7520 wytwarza trzy strumienie wizyjne o rozdzielczości Full HD, z kompresją cyfrową H.264/AVC. Moduł jest zgodny z ONVIF Profile S i Profile Q.

Głowicę ULISSE EVO można łatwo podłączyć do sieci Ethernet, aby przesyłać strumienie wizyjne do monitorów cyfrowych i systemów pamięci masowej.

Można ją zasilać, korzystając ze źródła prądu o napięciu 24 V_{AC}/24 V_{DC} lub metodą PoE, w zależności od wymagań instalacyjnych. Maksymalny pobór mocy wynosi 90 W.

Głowice mogą być montowane podstawą do dołu lub podstawą do góry, czyli w pozycji typowej dla kopułowych kamer szybkoobrotowych. Uchwyty montażowe mogą być wyposażone w łatwo rozłączalne złącza, dzięki którym można szybko zdemontować i wymienić uszkodzone głowice.

Standardowym wyposażeniem jest wycieraczka umożliwiająca oczyszczenie przedniej szyby. ULISSE EVO może pracować w temperaturze z zakresu od -40°C do 65°C. Obudowa jest zgodna ze standardami IK10 (odporność na udary mechaniczne), IP66, IP67, IP68, NEMA Type 4X i NEMA Type 6P (m.in. szczelność, odporność na korozję). Głowica jest odporna na działanie wiatru o prędkości do 230 km/h. Zapewnia to maksymalną ochronę modułu kamerowego przed kurzem i złą pogodą, silnymi podmuchami wiatru oraz aktami wandalizmu.

Bezpośr. inf. Videotec
www.videotec.com | sales@videotec.com

Tłumaczenie: Andrzej Walczyk
Redakcja

Kamery panoramiczne z modułem PTZ

Dzięki rozwojowi sprzętu stosowanego w systemach telewizji dozorowej uzyskujemy coraz lepsze przetworniki o coraz wyższej czułości lub większej rozdzielczości, wydajniejsze procesory sygnałowe i doskonalsze obiektywy. Ewolucja nie omija również konstrukcji kamer. Obecnie rosnącą popularnością cieszą się kamery posiadające więcej niż jedną matrycę, a otwarci na innowacje klienci potwierdzają coraz więcej możliwości ich wykorzystania.

Jednym z nieco bardziej konserwatywnych podejść do tematu jest stosowanie kamer obrotowych. Od lat nie zmieniono ich konstrukcji. Inne są tylko wykorzystywane podzespoły, czyli elementy składowe. Z jednej strony mamy rozwiązania nowoczesne, a z drugiej coś bardzo klasycznego i dobrze znanego.

Przykładem połączenia najnowszych trendów z konserwatywnymi koncepcjami jest konstrukcja kamery **DH-PSDW5631S-B360**. Jest to urządzenie wieloobiektywowe, które składa się z trzech przetworników o rozdzielczości 1920x1080, z obiektywami o ogniskowej 2,2 mm. Kamera jest wyposażona w promiennik IR o zasięgu 15 metrów. Moduł PTZ jest zbudowany z wykorzystaniem takiego samego przetwornika, jednakże zastosowano zmiennoogniskowy obiektyw o ogniskowej regulowanej w zakresie od 2,7 mm do 13,5 mm (kąt widzenia jest regulowany w zakresie od 105˚ do 33˚) i minimalnej przysłonie F1,8.

Kamery DH-PSDW5631S-B360 mają funkcje inteligentnej analizy obrazu, obsługują dwa strumienie wizyjne oraz mogą używać różnych algorytmów kompresji obrazu (H.265, H.264 oraz MJPEG w drugim strumieniu). Mają wszystkie popularne dziś funkcje – BLC, HLC, DWDR oraz funkcję zaawansowanej redukcji szumów. Kopuła stanowiąca obudowę kamery jest niewielka (zaledwie 172 mm średnicy). Dostępnych jest wiele akcesoriów umożliwiających montaż na różnych płaszczyznach. W efekcie możliwe jest stworzenie uniwersalnego punktu kamerowego wymagającego doprowadzenia tylko jednego przewodu.

Bezpośr. inf. Marian Maroszek
Dahua Technology Poland
Opracowanie: Redakcja

Xiaomi Mi Home Security Camera Basic

dobra kamera za niewielkie pieniądze

Wyroby firmy **Xiaomi** cieszą cię coraz większym uznaniem. Oprócz popularnych telefonów oraz przeróżnych przydatnych gadżetów Xiaomi zaprezentowało kamerę do monitorowania **Mi Home Security Camera Basic**. To małe i bardzo estetyczne urządzenie pasuje wyglądem do każdego wnętrza. Świetnie sprawdzi się w biurze, mieszkaniu, magazynie i wszędzie tam, gdzie potrzebny jest dozór wizyjny.

Mi Home Security Camera Basic nie tylko zapewnia wysokiej jakości obraz i dźwięk, ale także odznacza się wieloma użytecznymi funkcjami. Jedną z nich jest detekcja ruchu, dzięki której rejestrowane są tylko te zdarzenia, które są istotne ze względu na bezpieczeństwo obiektu. Warto również podkreślić wysoką jakość algorytmu detekcji ruchu. Jest on na tyle skuteczny, że potrafi odróżnić fałszywe alarmy powodowane zmianami oświetlenia lub ruchem zasłon okiennych od faktycznej obecności obiektów ruchomych w polu widzenia kamery.

Dzięki dwukierunkowej transmisji dźwięku można komunikować się głosowo z osobami przebywającymi w pobliżu kamery, a także nastraszyć komunikatem głosowym potencjalnego intruza.

Nagrania z kamery Xiaomi Mi Home Security Camera Basic mają bardzo wysoką jakość. Rozdzielczość obrazu to Full HD 1080p. Obiektyw kamery ma kąt widzenia równy 130°, dzięki czemu jedna kamera może służyć do obserwacji całego pomieszczenia. Kolejnym atutem są wbudowane diody LED pracujące w podczerwieni, które umożliwiają obserwację nawet w całkowitej ciemności, na odległość nawet dziesięciu metrów. Krótko mówiąc, dzięki Xiaomi Mi Home Security Camera Basic możliwa jest całodobowa ochrona obiektu.

Do podglądu obrazu służy aplikacja mobilna Mi Home, która jest intuicyjna w obsłudze. Niezwykła prostota oraz zrozumiałe funkcje ułatwiają sterowanie kamerą. Aplikację Mi Home dla użytkowników iPhone'a można pobrać ze sklepu Play lub iTunes.

Mi Home Security Camera Basic ma wbudowane gniazdo dla kart microSD, w którym można umieścić kartę o pojemności od 16 GB do 64 GB. Dzięki temu można mieć pewność, że wszystkie zdarzenia wychwycone dzięki detekcji ruchu zostaną zapisane na karcie pamięci.

Kamerę można nabyć przez Internet w sklepie www.batna24.com (https://www.batna24.com/pl/p/xiaomi-mi-home-security-camera-basic-1080p-kamera-ip-rmmkl). Urządzenie zostanie dostarczone w ciągu kilku dni.

Bezpośr. inf. Leszek Błaszczyk
www.batna24.com

BATNA24

Nowa wersja oprogramowania NMS AC

Oprogramowanie **NMS AC** jest intensywnie rozwijane. Ostatnio została udostępniona wersja 3.0. Aktualizacja jest dostępna na stronie produktu (https://nmsac.aat.pl/pl).

W nowej wersji dodano kilka opcji mających związek z integracją z systemem telewizji dozorowej. Umożliwiono otwarcie okna widoków zdefiniowanych uprzednio w zakładce *Szablony widoków*. W oknie można wyświetlać do 16 obrazów z kamer. Po kliknięciu na wybranym obrazie zostaje on wyświetlony na całym ekranie.

Nowa wersja oprogramowania umożliwia integrację systemu wizyjnego z systemem kontroli dostępu. Jeżeli nad czytnikiem kart identyfikacyjnych zainstalujemy kamerę skierowaną na twarz osoby stojącej przed czytnikiem, to w chwili odczytu karty zostanie zrobione zdjęcie, które następnie zostanie zapisane w bazie wraz z informacją o próbie uzyskania dostępu do danego przejścia. Na końcu opisu tego zdarzenia zostanie wyświetlona ikona aparatu. Po wskazaniu tej ikony kursorem myszy zostanie wyświetlane okno zawierające zdjęcie z formularza użytkownika, a obok zdjęcie zrobione w chwili odczytu karty. Umożliwia to zweryfikowanie, czy dana osoba użyła swojej karty dostępu.

W nowej wersji oprogramowania umożliwiono wyszukiwanie nowych kamer i rejestratorów NVR marki NOVUS w sieci LAN. Do tej pory automatyczne wyszukiwanie obejmowało tylko kontrolery. Dane na temat wyszukanych urządzeń są wyświetlane na liście w górnym oknie wyszukiwarki. Jeśli nowo wyszukane urządzenia są gotowe do dodania, z lewej strony ikony wyświetlany jest znak „+”. Jeśli występuje konflikt adresów, wyszukanych urządzeń nie można dodać do sieci IP. Urządzenia mające takie same adresy IP można bardzo szybko przeadresować, korzystając z opcji *Zaznacz z konfliktem IP* i *Zmień adres*, wpisując pierwszy adres z przydzielonej puli. Funkcja jest bardzo przydatna w przypadku nowych urządzeń, które mają ten sam fabryczny adres IP.

Nowe oprogramowanie automatycznie tworzy kopię danych dotyczących całego systemu. Odbywa się to zgodnie z terminarzem. Jest to bardzo ważna funkcja ze względu na serwis. Do tej pory tylko operator mógł stworzyć taką kopię.

Jeśli chcemy korzystać z typowego terminarza, np. obejmującego dni od poniedziałku do piątku i godziny od ósmej do siedemnastej, to nie musimy już podawać informacji dotyczących poszczególnych dni oddzielnie. Wystarczy podać dane na dole okna i zaznaczyć dni tygodnia, których one dotyczą. Dzięki temu operator może zaoszczędzić czas.

Polecam nową wersję oprogramowania wszystkim zainteresowanym. Kolejne ciekawe funkcje są w przygotowaniu.

Bezpośr. inf. Ryszard Sobierski
AAT HOLDING
Opracowanie: Redakcja

XX międzynarodowa konferencja IWMC

nt. gaszenia mgłą wodną odbędzie się w Polsce

Międzynarodowe stowarzyszenie IWMA ogłosiło, że konferencja IWMC 2020 odbędzie się **7 i 8 października 2020 r. w hotelu Regent w Warszawie**.

15 stycznia ogłoszone zostanie zaproszenie do zgłaszania referatów. Nieprzekraczalny termin składania streszczeń to 15 maja. Do 22 czerwca mówcy zostaną poinformowani, czy ich streszczenia zostały zaakceptowane. Wszystkie streszczenia zostaną ocenione przez Radę Naukową IWMA.

Internetowa strona konferencji i platforma rejestracyjna zostaną uruchomione 15 maja. IWMA będzie oferować obniżone ceny do 15 lipca.

Program zostanie opublikowany 1 lipca. Pierwszym dniem konferencji będzie Dzień Aplikacji. Uczestnictwo w tej części wydarzenia można zarezerwować osobno. Dzień drugi będzie poświęcony przede wszystkim naukowej stronie rozwiązań technicznych.

Biuro IWMA będzie przyjmować rezerwacje stoisk wystawowych od 15 stycznia.

Nieprzekraczalny termin nadsyłania zgłoszeń związanych z ubieganiem się o nagrodę IWMA Young Talent Award to 30 kwietnia. W tym roku nagroda ta trafi do autora najlepszej pracy magisterskiej dotyczącej mgły wodnej.

Bezpośr. inf. Bettina McDowell
tel.: +49 (0) 40 35085-215
faks: +49 (0) 40 35085-80
e-mail: mcdowell@iwma.net
www.iwma.net

Prowadzącymi konferencję IWMA są W. Brandt, IWMA Young Talent – Topi Sikanen i przewodniczący rady naukowej IWMA – Hong-Zeng Yu.

Panel dyskusyjny będzie dotyczył pożaru w katedrze Notre Dame i tego, w jaki sposób systemy gaszące mgłą wodną zapobiegają utracie życia, mienia i miejsc pracy.

Tłumaczenie: Redakcja

Zabezpiecz swój sukces

Przed nami 23. edycja Międzynarodowych Targów Zabezpieczeń SECUREX, które odbędą się 21-23 kwietnia 2020 r. Producenci oraz dystrybutorzy zaprezentują w Poznaniu najnowsze rozwiązania i premiery produktowe w segmentach monitoringu, kontroli dostępu, systemów alarmowych, ochrony informacji, mienia, rozwiązań smart building, jak również wszelkich zabezpieczeń - od tych mechanicznych po systemy IT.

Targi Securex są największym w Europie Środkowo-Wschodniej wydarzeniem branży zabezpieczeń.
To miejsce bezpośredniego kontaktu przedstawicieli branży, zarówno dostawców jak i firm oferujących wdrożenia i usługi z zakresu zabezpieczeń, klientów biznesowych, inwestorów prywatnych i instytucjonalnych, przedstawicieli służb i ekspertów. Dzięki ekspozycji na Międzynarodowych Targach Poznańskich będzie można poznać z bliska i przetestować innowacje technologiczne, a także porozmawiać o ich możliwościach. Bogaty program wydarzeń towarzyszących – konferencji, otwartych prelekcji i debat, a także niezwykle atrakcyjnych pokazów specjalnych, pozwoli poszerzyć wiedzę oraz zainspiruje do implementacji i integracji najnowocześniejszych systemów służących bezpieczeństwu.

Doświadczenie i współpraca „w akcji"
Fachowe umiejętności i doświadczenie instalatorów oraz służb będzie można podziwiać podczas VII Mistrzostw Polski Instalatorów Systemów Alarmowych organizowanych wspólnie z Polską Izbą Systemów Alarmowych oraz Mistrzostw Polskiej Izby Ochrony w Strzelectwie, na które zaprasza Polska Izba Ochrony. PIO przygotowuje również pokazy skutecznej interwencji służb ochrony oraz debatę na temat bezpieczeństwa imprez masowych. Wielkopolska Policja udostępni autentyczną dyspozytornię systemu powiadamiania ratunkowego 112, w której będzie można sprawdzić się w roli dyspozytora. Funkcjonariusze zaprezentują także interwencje z wykorzystaniem wyszkolonych psów, które odegrają kluczową rolę w zatrzymaniu groźnego przestępcy oraz wykrywaniu substancji niedozwolonych.

Eksperci do dyspozycji
Współpraca Targów Securex z partnerami zrzeszającymi ekspertów i liderów poszczególnych sektorów branży zaowocuje możliwością uzyskania specjalistycznego doradztwa. Krajowe Stowarzyszenie Ochrony Informacji Niejawnych oraz Stowarzyszenie Wspierania Bezpieczeństwa Narodowego zorganizują punkty konsultacyjne w zakresie: ochrony informacji niejawnych, biznesowych, danych osobowych oraz zarządzania kryzysowego i ochrony infrastruktury krytycznej. Ogólnopolskie Stowarzyszenie Inżynierów i Techników Zabezpieczeń Technicznych i Zarządzania Bezpieczeństwem POLALARM i zaproszą do konsultacji z rzeczoznawcami w zakresie technicznej ochrony osób i mienia oraz zarządzania bezpieczeństwem. Zagadnienia z zakresu zabezpieczeń IT podejmą przedstawiciele Stowarzyszenia Ekspertów Bezpieczeństwa.

Wspólnie dla bezpieczeństwa, infrastruktury i środowiska
Kwietniowy blok targów to najważniejsze wydarzenie biznesowe skierowane do profesjonalistów z kilku branż technicznych. Najnowsze rozwiązania i produkty na Międzynarodowych Targach Poznańskich zaprezentuje łącznie kilkuset wystawców w ramach ekspozycji Międzynarodowych Targów Zabezpieczeń Securex, a także: Międzynarodowych Targów Instalacyjnych INSTALACJE, Poznań Drone Expo, Międzynarodowych Targów Ochrony Pracy, Pożarnictwa i Ratownictwa SAWO, Międzynarodowych Targów Energii Odnawialnej GreenPOWER oraz Międzynarodowych Targów Energetyki EXPOPOWER. Podczas trzech dni w imprezie weźmie udział około 30 tysięcy profesjonalistów.

Zainstaluj się w strefie fachowców!
www.securex.pl

Transformacja systemów bezpieczeństwa – konieczność czy szansa?

Podsumowanie konferencji

W listopadzie 2019 r. Polski Związek Pracodawców Ochrona zorganizował konferencję pt. *Transformacja systemów bezpieczeństwa – konieczność czy szansa?*.

Spotkanie odbyło się w centrum Warszawy w **Centre Business Club**, a gości powitał Tomasz Wojak – prezes Polskiego Związku Pracodawców Ochrona. W konferencji wzięło udział około 120 osób, w tym przedstawiciele kadry menedżerskiej firm ochrony i firm partnerskich PZPO. Konferencja była podzielona na pięć paneli tematycznych.

Omówiono m.in. zmiany legislacyjne dotyczące kosztów pracy i ubezpieczeń społecznych, warunki zatrudniania cudzoziemców i obecną sytuację na rynku pracy w branży ochrony. Zbyt mała liczba pracowników oraz wciąż rosnące koszty ich zatrudnienia wymuszają na firmach korzystanie z alternatywnych rozwiązań.

Na spotkaniu mówiono także o rozwoju techniki oraz o rozwiązaniach biznesowych przeznaczonych do wykorzystania w przemyśle i handlu, które umożliwią optymalizację kosztów ochrony obiektu.

Przedstawiono korzyści płynące z automatyzacji różnych procesów, np. z rejestracji gości i pojazdów, z zastosowania systemów do zarządzania bezpieczeństwem w obiektach rozproszonych, z wykorzystania robotów, dronów oraz systemów monitorowania i kontroli dostępu.

Omówiono również elementy systemu bezpieczeństwa centrum handlowego. Spotkanie zakończyło się dyskusją na temat przyszłości usług ochrony.

Patronat honorowy nad konferencją objęły Polska Organizacja Handlu i Dystrybucji, Federacja Przedsiębiorców Polskich oraz Polska Rada Centrów Handlowych.

Zapraszamy do obejrzenia fotorelacji z wydarzenia (https://www.zabezpieczenia.com.pl/fotogalerie).

Bezpośr. inf. Ela Końka

4 grudnia 2019 r.

zmarł Jacek Szewczyk

właściciel firmy Compas

Jacek Szewczyk po raz pierwszy zetknął się z branżą zabezpieczeń już w technikum elektronicznym. Kilka lat później, wraz z Włodzimierzem Lechem, instalował systemy alarmowe w domach jednorodzinnych i mieszkaniach. W latach 1985-1986 w wynajętym garażu w Babicach Starych k. Warszawy rozpoczął produkcję urządzeń do systemów alarmowych. W roku 1989 wraz z żoną Anną spełnił swoje marzenie i przeniósł firmę do nowej siedziby w Jabłonnie k. Warszawy. Obecnie pracuje tam 12 osób, w tym również ich córka i syn, zatem firma ma charakter rodzinny. W Jabłonnie powstał pierwszy polski system kontroli dostępu.

Jacek utrzymywał serdeczne kontakty z ludźmi z branży, był zawsze chętny do pomocy, miał niebanalne poczucie humoru i nieustającą gotowość do zabawy. Zawsze robił wszystko na swoich warunkach. Odszedł, chociaż tak bardzo kochał życie.

Redakcja czasopisma „Zabezpieczenia" składa wyrazy głębokiego współczucia rodzinie i bliskim Jacka.

Sprawozdanie
III Ogólnopolski Kongres Naukowo-Techniczny
SAFE PLACE 2019

Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej

Dobre praktyki cywilne i wojskowe

W dniach 19-20 listopada 2019 roku w Hotelu Windsor w Jachrance k. Warszawy odbył się trzeci **Ogólnopolski Kongres Naukowo-Techniczny SAFE PLACE 2019 Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. *Dobre praktyki cywilne i wojskowe***. To cykliczne wydarzenie na stałe wpisało się w kalendarz spotkań teoretyków i praktyków z zakresu bezpieczeństwa antyterrorystycznego. Grono uczestników w porównaniu do lat przeszłych zwiększyło się, co świadczy o merytorycznej sile wydarzenia, które rok rocznie przyciąga swym całokształtem nowe instytucje do współpracy. Ponadto trzecia edycja SAFE PLACE poszczycić się może patronatem honorowym Dyrektora Rządowego Centrum Bezpieczeństwa oraz wsparciem merytorycznym ze strony Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego i DG Home Komisji Europejskiej.

Organizatorzy wydarzenia, czyli Uniwersytet Wrocławski – Zakład Socjologii Edukacji Instytutu Socjologii, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego Apeiron w Krakowie oraz Safety Project Stelmach Jarosław – od początku istnienia Kongresu SAFE PLACE dokładają wszelkich starań, by osiągnąć jak najwyższy poziom merytoryczny i organizacyjny wydarzenia. Jest to możliwe dzięki współpracy z instytucjami naukowymi, które pełniły rolę współorganizatorów naukowych, spośród których należy wymienić Wyższą Szkołę Policji w Szczytnie, Instytut Politologii Uniwersytetu Opolskiego, Wydział Nauk o Polityce i Administracji Uniwersytetu Kazimierza Wielkiego w Bydgoszczy, Wyższą Szkołę Bankową we Wrocławiu oraz Zakład Socjologii Grup Dyspozycyjnych Uniwersytetu Wrocławskiego. Grono naukowe tychże instytucji stanowiło istotny głos w debacie na tematy podejmowane w trakcie Kongresu. Kluczowym było także wsparcie ze strony współorganizatorów instytucjonalnych, do grona których należeli: Służba Ochrony Państwa, Komenda Stołeczna Policji, Oddział Specjalny Żan-

darmerii Wojskowej w Warszawie, Samodzielny Poddział Kontrterrorystyczny Policji w Warszawie, Polskie Sieci Elektroenergetyczne S.A., Polskie Koleje Państwowe S.A., Polska Izba Ochrony, Polska Izba Systemów Alarmowych, Związek Banków Polskich, Polskie Towarzystwo Bezpieczeństwa Narodowego oraz firma UTC Fire & Security. Co ważne, w roli ekspertów udział wzięli przedstawiciele Centrum Antyterrorystycznego (CAT ABW) oraz Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego (CPT ABW), DG Home Komisji Europejskiej oraz Polskiego Komitetu Normalizacyjnego. Patronat medialny nad wydarzeniem objęli: Wydawnictwo Adam Marszałek, Wydawnictwo DIFIN, Magazyn *Zabezpieczenia*, Grupa Wydawnicza Euro-Media – czasopismo – *Ochrona Mienia i Informacji*, Defence24.pl, InfoSecurity24.pl, Special OPS oraz Alarmy.org.

Trzeci Kongres SAFE PLACE kontynuując założenia poprzednich edycji, był okazją do skonfrontowania wiedzy teoretycznej z zakresu bezpieczeństwa antyterrorystycznego z praktycznymi rozwiązaniami technicznymi. By było to możliwe, wydarzenie przebiegało w formie paneli tematycznych, debat eksperckich, dyskusji oraz prezentacji sprzętu technicznego, których dokonali przedstawiciele firm wiodących na rynku polskim i zagranicznym. Dzięki zaangażowaniu organizacyjnemu Oddziału Specjalnego Żandarmerii Wojskowej w Warszawie, Samodzielnego Pododdziału Kontrterrorystycznego Policji w Warszawie oraz Służby Ochrony Państwa, uczestnicy mogli zapoznać się z najnowocześniejszym sprzętem i uzbrojeniem kontrterrorystycznym wykorzystywanym podczas zadań specjalnych.

SAFE PLACE 2019 skupił się na kilku elementarnych obszarach z zakresu bezpieczeństwa antyterrorystycznego. Po pierwsze, poruszono kwestie ochrony infrastruktury krytycznej oraz obiektów podlegających obowiązkowej ochronie. Odwołano się także do problematyki dotyczącej bezpieczeństwa banków oraz innych obiektów sektora finansowego. Ponadto w związku z zaangażowaniem się w organizację Kongresu Polskich Kolei Państwowych, oddzielną sesję zadedykowano bezpieczeństwu na obszarach kolejowych.

W ramach różnotematycznych paneli wystąpili przedstawiciele instytucji naukowych oraz bezpieczeństwa publicznego, odwołując się do wymiaru teoretycznego oraz praktycznego. Tematyka wystąpień została podsumowana i rozbudowana podczas debat eksperckich, kończących każdą sesję. Udział wzięli w niej eksperci z dziedziny bezpieczeństwa antyterrorystycznego, m.in. przedstawiciele Służby Ochrony Państwa, Komendy Stołecznej Policji, Polskich Sieci Elektroenergetycznych S.A., CPT ABW oraz Polskiego Komitetu Normalizacyjnego.

Kongres SAFE PLACE 2019 przeszedł do historii, natomiast treści merytoryczne z obrad uwiecznione zostały w materiale filmowym, który będzie opublikowany na kanale Safety Project You Tube. Dodatkowo jak co roku pod koniec roku zostanie wydana publikacja zawierająca szereg tekstów naukowo – praktycznych z obszaru bezpieczeństwa budynków użyteczności publicznej. Organizatorzy Safe Place ciesząc się wspólnym sukcesem już teraz zapraszają na kolejną edycję wydarzenia, tym razem o charakterze międzynarodowym. Niezmiernie miło nam poinformować, iż **SAFE PLACE 2020 IV Międzynarodowy Kongres Naukowo-Techniczny *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej dobre praktyki - wymiar międzynarodowy i krajowy*** odbędzie się w dniach 19-21 października 2020 roku w Hotelu Windsor w Jachrance k. Warszawy. Swoją obecność potwierdzili światowej klasy eksperci z USA, Izraela oraz obszaru Unii Europejskiej, co podniesie wydarzenie do rangi światowej.

mjr rez. dr inż. Jarosław Stelmach - Przewodniczący Komitetu Organizacyjnego Kongresu

Malwina Wach – Członek Komitetu Organizacyjnego Kongresu, Safety Project

Kontakt: konferencja@safetyproject.pl
tel. 531 419 151, http://safetyproject.pl/

Obejrzyj film z Kongresu SAFE PLACE 2019:
https://www.youtube.com/watch?v=S5We2YmI-00Q&t=142s

Zapraszamy do obejrzenia fotorelacji:
https://www.zabezpieczenia.com.pl/fotogalerie

Nowe produkty i rozwiązania w systemach kontroli dostępu

Nowa klamka elektroniczna
do systemu blueSmart

Asortyment komponentów systemu **Winkhaus blueSmart**, które mają różne zastosowania, jest szeroki. Najnowsza propozycja to inteligentna klamka elektroniczna **ETB-IM**, która jest dostępna od tego roku.

Dzięki zainstalowaniu elektronicznej klamki ETB-IM w drzwiach wewnętrznych można szybko i w nieskomplikowany sposób rozbudować istniejący system kontroli dostępu lub stworzyć nowy. Nowa klamka zapewnia całkowitą kompatybilność z produktami blueSmart. Jest przystosowana do wszystkich popularnych drzwi wewnętrznych – z drewna, stali lub tworzywa sztucznego o różnych grubościach.

Bezprzewodowa klamka elektroniczna ma wiele zastosowań. Można ją zainstalować np. w drzwiach wewnętrznych z zamkiem wpuszczanym z funkcją zapadki lub samoryglującym zamkiem automatycznym. Do szybkiej bezdotykowej komunikacji służą specjalne breloki do kluczy, karty identyfikacyjne i klucze blueSmart. Sprawdzanie uprawnień odbywa się po zewnętrznej stronie drzwi, a od wewnątrz wystarczy nacisnąć klamkę, by otworzyć drzwi. Dzięki funkcji pojedynczego lub stałego otwarcia (ustawianej ręcznie lub automatycznie) można bardzo elastycznie zarządzać dostępem do pomieszczeń w obiekcie.

Elektroniczna klamka drzwiowa może w razie potrzeby zostać połączona z wkładką mechaniczną lub elektroniczną, np. w celu przydzielenia specjalnych uprawnień lub otwarcia drzwi w sytuacji alarmowej.

Komponenty są zmontowane fabrycznie, dlatego ich instalacja w drzwiach jest bardzo prosta: – po zdemontowaniu dotychczasowej klamki należy przykręcić klamkę elektroniczną (zabezpieczając ją jednocześnie przed przekręceniem). Wykorzystuje się w tym celu odpowiednie otwory w zamku. Odbywa się to bez dodatkowego okablowania, uszkodzenia skrzydła drzwiowego, a często także bez nawiercania. Proces montażu pokazuje instrukcja szybkiej instalacji oraz animacja komputerowa. Równie szybko, za pomocą standardowych narzędzi można dokonać zmiany kierunku działania klamki oraz wymiany baterii.

W ofercie jest pięć modeli klamek do drzwi standardowych, z których trzy są dopuszczone do stosowania także w drzwiach ewakuacyjnych zgodnych z normą EN 179. Wygląd i materiał, z którego wykonano klamki, są dostosowane do różnych typów obiektów. Uchwyty są wykonane ze stali nierdzewnej o wysokiej jakości. Dzięki dyskretnym obudowom z tworzywa sztucznego w kolorze czarnym lub białym klamki pasują do niemal każdego budynku.

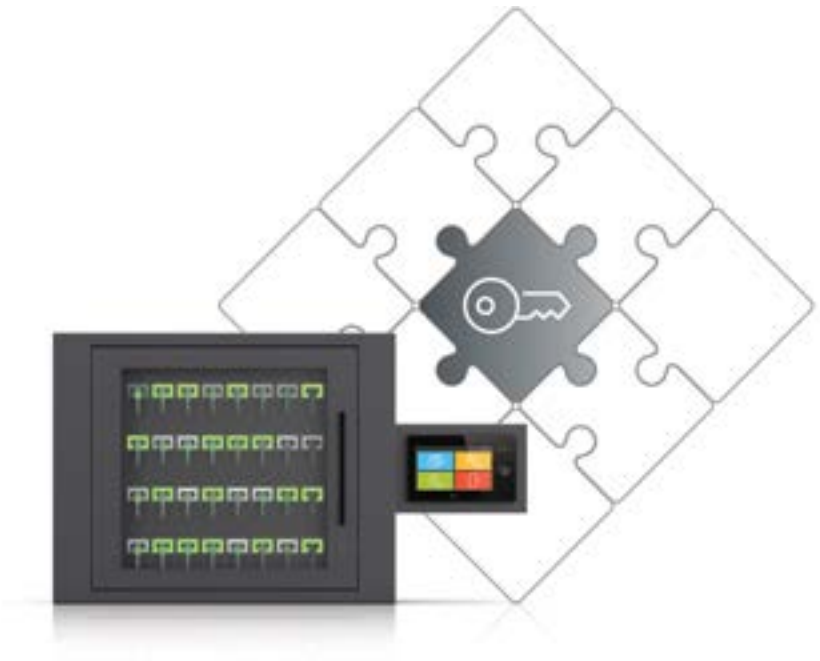
Bezpośr. inf. Klaudia Mendyka-Waszkowiak
Winkhaus Polska

Serwisowy kontroler dostępu MC16-SVC

Kontroler **MC16-SVC** jest urządzeniem kompatybilnym z kontrolerami dostępu z serii **MC16** i jest przeznaczony do wykorzystania jako urządzenie demonstracyjne lub serwisowe. Kontroler MC16-SVC jest dostarczany z kompletem tzw. licencji serwisowych, które umożliwiają przełączenie go w tryb pracy zgodny z dowolną odmianą kontrolera serii MC16. Przede wszystkim może on zostać skonfigurowany w taki sposób, by pracować jako kontroler dostępu do 16 przejść (MC16-PAC-16), kontroler szafkowy do obsługi 64 szafek (MC16-LRC-64) lub kontroler klasycznej windy przystosowanej do obsługi 64 pięter (MC16-EVC-64). Aby kontroler pracował w danym trybie, należy wybrać odpowiednią licencję serwisową, a w niektórych przypadkach także wyposażyć go w potrzebną wersję oprogramowania. Czas pracy kontrolera na licencji serwisowej jest ograniczony do dziesięciu dni i jest liczony od daty początkowej zapisanej przez instalatora w pliku konfiguracyjnym na karcie pamięci. Po upływie okresu ważności tej licencji kontroler samoczynnie wstrzymuje normalną pracę. W celu ponownego umożliwienia jego pracy konieczne jest wpisanie w pliku konfiguracyjnym nowej daty początkowej. Czas pracy kontrolera może być przedłużany dowolną liczbę razy. Można go przedłużyć także z wyprzedzeniem – przed upływem okresu ważności. Możliwe jest zamówienie licencji komercyjnej umożliwiającej bezterminowe korzystanie z kontrolera serwisowego zastępującego inne urządzenie, które uległo uszkodzeniu i zostało wysłane do naprawy. Kontroler serwisowy jest oferowany jako niezależny moduł elektroniczny oraz jako element zestawów demonstracyjnych z serii DB oraz PDK. Opcjonalnie kontroler może być skonfigurowany w taki sposób, by pracować w trybie demonstracyjnym. W tym przypadku pracuje normalnie w godzinach 6–22, a poza tymi godzinami nie działa. Tryb demonstracyjny jest bezterminowy i nie wymaga zmiany daty początkowej.

Bezpośr. inf. ROGER

Integracja depozytora kluczy RKD32
z systemem RACS 5



W związku z zapotrzebowaniem do systemu kontroli dostępu i automatyki budynkowej **RACS 5** dodano obsługę depozytorów kluczy z serii **RKD** firmy **ROGER**. Dzięki temu możliwe jest obecnie kompleksowe zarządzanie depozytorami kluczy oraz monitorowanie ich obiegu z poziomu oprogramowania zarządzającego systemem kontroli dostępu. Według przyjętej koncepcji użytkownicy systemu kontroli dostępu stają się automatycznie użytkownikami depozytorów kluczy, a klucze stają się wyposażeniem zarządzanym z poziomu systemu kontroli dostępu. Dostęp użytkowników do kluczy podlega regulacjom według identycznych zasad jak uprawnienia użytkowników do przejść czy do korzystania z innych funkcji dostępnych w systemie RACS 5. Użycie jednolitych reguł zarządzania dostępem do przejść, kluczy i innych elementów wyposażenia budynku jest dużym ułatwieniem dla obsługi obiektu ze względu na ograniczenie wymaganej wiedzy, a także możliwość obsługi systemu z jednego miejsca. Program zarządzający VISO do systemu RACS 5 umożliwia zarządzanie wieloma depozytorami kluczy. Zarządzanie depozytorami kluczy z poziomu oprogramowania do systemu kontroli dostępu jest możliwe także wówczas, gdy obiekt nie jest wyposażony w system kontroli dostępu. W takim przypadku program VISO staje się platformą przeznaczoną wyłącznie do obsługi systemu depozytorów kluczy. Integracja depozytorów kluczy jest możliwa w zaawansowanej wersji systemu (RACS 5 EX), jak również w wersji standardowej (RACS 5 ST), przy czym w przypadku tej drugiej wymagana jest odpłatna licencja. Integracja depozytorów kluczy z systemem kontroli dostępu jest kolejnym krokiem na drodze do celu, jakim jest kompleksowe zarządzanie budynkiem z wykorzystaniem jednolitego oprogramowania do obsługi systemu kontroli dostępu i automatyki budynkowej RACS 5.

Bezpośr. inf. ROGER

Dobór certyfikowanej stolarki budowlanej do kontrolowanych przejść

Sławomir Goździecki

Ostatnio dyskutuje się o tym, co można, a czego nie można stosować jako elementy służące do ryglowania drzwi o określonej odporności na włamanie, objętych działaniem systemu kontroli dostępu. Odporność tę zdefiniowano w normie PN-EN 1627 *Drzwi, okna, ściany osłonowe, kraty i żaluzje. Odporność na włamanie. Wymagania i klasyfikacja*

Proponowane są elektrozaczepy, zwory, rygle, elektrorygle. Możliwe jest też zastosowanie zamków jako jedynego zabezpieczenia. Jeśli mają być użyte zamki, to ile powinno ich być? Jeden, dwa, a może jeden zamek wielopunktowy? Wiadomo, że jeśli stolarka o określonej odporności na włamanie została przebadana w procesie certyfikacji razem z konkretnym wyposażeniem, np. zamkiem odpowiedniej klasy, to nie można ani zastosować zamka innej klasy, ani dokonywać jakichkolwiek przeróbek tego produktu, np. poprzez wyposażenie go w zwory lub elektrozaczepy.

Pomimo wspomnianych trudności, systemy kontroli dostępu są jednak powszechnie stosowane. Jest to podyktowane względami bezpieczeństwa i wygody użytkowania budynków. Jak więc postąpić, gdy ze względów bezpieczeństwa konieczne jest zastosowanie certyfikowanych drzwi? Nie jest to trudne, jednak należy przestrzec kilku zasad.

Pamiętając o złotej zasadzie ochrony obiektów, a mianowicie o tym, że czas jest najważniejszy, należy odpowiednio dobrać zabezpieczenia budowlane, w tym mechaniczne, wszędzie tam, gdzie potrzebna jest kontrola dostępu. Drzwi, o których mowa powyżej, muszą być badane razem z elementami mechanicznymi, do których należą zamki. Niepodważalną zasadą jest zatem wybranie wyrobu przebadanego przez akredytowaną jednostkę certyfikującą. Dzięki temu wyrób będzie miał wbudowane odpowiednie zabezpieczenia mechaniczne. W normie PN-EN 1627 określono, jakiej klasy wyposażenia należy użyć, aby spełnione były minimalne wymogi dotyczące zabezpieczeń budowlanych odpowiedniej klasy.

Czas jest najważniejszy.
To złota zasada ochrony.
Na skuteczność ochrony wpływa:
– czas interwencji (ochrona fizyczna),
– czas alarmu (ochrona techniczna),
– czas oporu (ochrona budowlana/mechaniczna).

Kolejnym obowiązkowym elementem wyposażenia drzwi określonym w normie PN-EN 1627 są certyfikowane okucia, takie jak wkładki bębenkowe, tarcze drzwiowe oraz zamki.

Zgodnie z normą PN-EN 1627 w certyfikowanych drzwiach nie wolno stosować zabezpieczeń mechanicznych, takich jak zwory, elektrozaczepy, elektrorygle, i jakichkolwiek innych okuć poza wymienionymi w normie. Oczywiście można zastosować system kontroli dostępu w przypadku drzwi odpowiedniej klasy, wyposażonych w zamek lub zamki spełniające wymogi określone w normie PN-EN 1627, a także w zworę, jednak takie rozwiązanie wymaga ryglowania drzwi zarówno przez zamki, jak i przez zworę. Otwieranie i zamykanie za pomocą karty drzwi, które są zamykane także na zamki za pomocą kluczy mechanicznych, wydaje się mało komfortowe. Jak rozwiązać ten problem? To proste. Należy zastosować certyfikowane drzwi, które są fabrycznie przystosowane do współpracy z systemem kontroli dostępu. Takie rozwiązanie daje nam pewność, że drzwi zostały przebadane pod kątem zgodności z normą PN-EN 1627 razem z fabrycznym wyposażeniem.

Na rynku dostępne są certyfikowane drzwi, które mogą współpracować zarówno z systemami kontroli dostępu różnych producentów (ponieważ są fabrycznie wyposażone w odpowiednie zamki elektryczne lub elektromotoryczne), jak i z systemami sygnalizacji włamania i napadu (ponieważ są fabrycznie wyposażone w czujniki otwarcia spełniające wymagania dotyczące trzeciego stopnia zabezpieczenia). Takie rozwiązanie jest nie tylko wygodne, ale również bezpieczne, ponieważ alarm włączy się nie po otwarciu drzwi, ale znacznie wcześniej, już przy próbie włamania poprzez penetrację, zgodnie z PN-EN 50131-1 *Systemy alarmowe. Systemy sygnalizacji włamania i napadu. Cz. 7: Wytyczne stosowania*. Ten wymóg obowiązkowo dotyczy trzeciego i czwartego stopnia zabezpieczenia.

Należy uważnie dobrać stolarkę budowlaną o odpowiedniej szczelności ogniowej E i izolacyjności ogniowej I. Należy zaoferować gotowe certyfikowane drzwi, które będą charakteryzować się odpowiednią odpornością ogniową.

Nie zapominajmy, że drzwi na drogach ewakuacyjnych muszą zagwarantować swobodę przejścia w warunkach panujących w czasie pożaru. Także w tym przypadku rozwiązaniem jest zastosowanie drzwi fabrycznie przystosowanych do współpracy z systemami kontroli dostępu. Takie drzwi będą wygodne w użyciu i umożliwią bezpieczną ewakuację z wykorzystaniem klamek lub dźwigni antypanicznych, które służą do mechanicznego otwarcia drzwi, do którego nie używa się klucza i w przypadku którego system sygnalizacji pożarowej nie steruje zamknięciem. Możliwe jest fabryczne przystosowanie drzwi zarówno do jednostronnej, jak i do dwustronnej kontroli przejścia.

Co należy zrobić, jeśli drzwi o odpowiedniej odporności włamaniowej i pożarowej są już zainstalowane i chcemy zastosować system kontroli dostępu? Można zastosować najnowsze rozwiązania, takie jak wkładki i klucze programowalne (kontrola dostępu w kluczu). Takie rozwiązanie zapewni wygodę użytkowania, którą daje system kontroli dostępu, i jednocześnie zachowanie bardzo wysokiego poziomu zabezpieczenia mechanicznego dzięki zastosowaniu cylindrów we wkładce. Dodatkowo daje możliwość grupowania przejść w systemie klucza generalnego, zarówno w wersji elektronicznej, jak i mechanicznej. System ten jest stale rozbudowywany i poza znanym do tej pory rozwiązaniem polegającym na pobieraniu danych uprawniających do dostępu z naściennego lub mobilnego programatora pojawiły się rozwiązania wykorzystujące łącza Bluetooth oraz IP. Te dwie ostatnie metody wykorzystują zwykły smartfon do pobierania danych dostępowych. W metodzie IP dane z systemu i z bazy danych są wymieniane w czasie rzeczywistym, przez co zachowany jest taki poziom zabezpieczeń jak w systemach kontroli dostępu o wysokim poziomie zabezpieczenia.

Sławomir Goździecki
Energo-Security Serwis
e-mail: slawomir.gozdziecki@ess24.pl

RACS 5

System kontroli dostępu klasy *Enterprise*

Przewodowa kontrola dostępu

Bezprzewodowa kontrola dostępu

Rejestracja czasu pracy

Automatyka budynkowa

Zarządzanie kluczami

Identyfikacja mobilna

roger®
Intelligence for Building

WYRÓB POLSKI

Kontrola dostępu i automatyka do hoteli
w ofercie firmy ROGER

Grzegorz Wensker

Elektroniczne systemy kontroli dostępu mają zastosowanie między innymi w obiektach hotelowych. W hotelach często stosowane są zasilane bateryjnie zamki mechatroniczne działające autonomicznie, bez połączenia z serwerem zarządzającym. Z reguły działanie systemów tego typu ogranicza się do kontroli dostępu. Alternatywą dla bateryjnych zamków mechatronicznych są przewodowe systemy kontroli dostępu. Oprócz kontroli dostępu takie systemy oferują także mniej lub bardziej zaawansowane funkcje automatyki budynkowej. W ofercie firmy ROGER znajdują się obydwa te rozwiązania, które zostaną pokrótce omówione

Bateryjne zamki mechatroniczne

Tego typu zamki mają ogromną zaletę. Ich zainstalowanie zwykle sprowadza się do wykonania drobnych prac monterskich w skrzydle drzwiowym i – co bardzo ważne – nie ma konieczności wykonywania jakiegokolwiek dodatkowego okablowania. W przypadku tego typu zamków do potwierdzania tożsamości przez użytkowników służą zwykle karty zbliżeniowe lub – rzadziej – magnetyczne. Prawa do dostępu są zapisane na karcie dostępowej. Oprócz informacji o tym, które przejścia można daną kartą otworzyć, zwykle zapisany jest także termin jej ważności.

Fot. 1. Zamki bezprzewodowe systemu RACS 5 AIR

Osobną grupę stanowią zamki wyposażone w radiowe interfejsy komunikacyjne. Zamki te są bardziej zaawansowane

pornnikau - stock.adobe.com

technicznie i przez to droższe. W systemach, w których wykorzystywana jest komunikacja radiowa, możliwe jest uzyskanie identycznych funkcji jak w systemach przewodowych. Możliwe jest monitorowanie działania systemu oraz sprawne zarządzanie uprawnieniami dostępowymi z poziomu oprogramowania. W przypadku bateryjnych zamków z komunikacją radiową konieczne jest rozmieszczenie w budynku sieci przewodowych punktów dostępowych, które zwykle muszą się znajdować w odległości nie większej niż kilka metrów od zamka, z którym współpracują. W zależności od systemu punkty dostępowe mogą obsługiwać od jednego do kilku zamków. Radiowe zamki bezprzewodowe zwykle wykorzystują pasmo 2,4 G współdzielone z siecią Wi-Fi. Z tego powodu istnieje zagrożenie nieumyślnym lub umyślnym działaniem, które zakłóci łączność radiową, dlatego zamki tego typu zwykle mogą pracować w trybie awaryjnym, w którym dostęp jest przyznawany zgodnie z uproszczonymi regułami – często na podstawie listy kart, która jest na stałe lub dynamicznie zapisana w pamięci elektronicznej zamka.

Fot. 2. Terminale hotelowe systemu RACS 5

Przewodowe systemy kontroli dostępu

Każdy z oferowanych obecnie przez firmę ROGER systemów kontroli dostępu (RACS 4 i RACS 5) ma funkcje stworzone z myślą o zastosowaniach hotelowych. Nie chodzi jednak o szerokie spektrum specyficznych funkcji oczekiwanych w obiektach hotelowych, lecz raczej o niedrogie rozwiązania zapewniające minimum koniecznych funkcji związanych z kontrolą dostępu i ewentualnie z podstawową automatyką. W ofercie firmy znajduje się również grupa urządzeń przeznaczonych do zastosowań hotelowych, w skład której wchodzą kontrolery z serii HRC oraz terminale dostępu i panele sterowania z serii HRT. Zakres funkcji tych urządzeń spełni nawet najwyższe wymagania.

Systemy przewodowe znajdują zastosowanie głównie w nowych obiektach, w których ułożenie kabli nie stwarza istotnych problemów, a zastosowanie urządzeń przewodowych umożliwia zaawansowane funkcje, a w efekcie duży komfort użytkowania.

Wykorzystanie systemów RACS 4 i RACS 5 w hotelach

System RACS 4 w hotelach umożliwia kontrolę dostępu do pokoi i w przejściach publicznych. W ramach automatyki możliwe jest sterowanie zasilaniem elektrycznym w pokojach oraz zapewnienie sygnalizacji hotelowej (*Nie przeszkadzać*, *Posprzątać* itp.). Kontrolerem może być standardowe urządzenie z serii PR lub przeznaczony do wykorzystania w hotelu kontroler PR821-CH umieszczony w obudowie czytnika z kieszenią na kartę zbliżeniową.

System RACS 5 oferuje znacznie większy zakres funkcji przeznaczonych do wykorzystania w hotelu niż RACS 4, a dodatkowo udostępnia tzw. serwer integracji, co stanowi bardzo istotny walor. Oprogramowanie tego serwera umożliwia integrację programową systemu kontroli dostępu RACS 5 z oprogramowaniem zarządzającym hotelem, a w szczególności z oprogramowaniem używanym w recepcji. Dzięki serwerowi integracji

Fot. 3. Terminale hotelowe serii HRT

możliwe jest także realizowanie dodatkowej, nieistniejącej oryginalnie, logiki działania systemu, a zaimplementowanej w zewnętrznym oprogramowaniu wykonanym pod konkretny projekt. Oprócz sterowania zasilaniem elektrycznym w pokojach hotelowych oraz sygnalizacją hotelową RACS 5 umożliwia sterowanie oświetleniem z użyciem scen świetlnych, a także monitorowanie statusu pokoju z poziomu oprogramowania zarządzającego systemem. System może służyć do kontrolowania dostępu do pokoi hotelowych, w przejściach wspólnych, do wind i parkingu, a wszystko to za pomocą tego samego oprogramowania zarządzającego.

Wykorzystanie urządzeń z serii HRC i HRT w hotelach

W ofercie firmy ROGER znajdują się kontrolery dostępu i automatyki HRC102DR i HRC402DR, które zostały stworzone specjalnie z myślą o obiektach hotelowych. Kontrolery te mogą współpracować z urządzeniami peryferyjnymi, do których należą czytniki korytarzowe, kieszenie na kartę, panele sterujące ogólnego i specjalnego przeznaczenia, panele sterowania klimatyzacją oraz ekspandery linii we/wy. Urządzenia te są dostępne w wersji podtynkowej i natynkowej. Są wyposażone w szklane panele frontowe. Panele te są trwałe i estetyczne, co jest szczególnie istotne w przypadku urządzeń hotelowych. Kontrolery z serii HRC umożliwiają kontrolę dostępu do pomieszczeń wspólnych oraz pokoi gościnnych, a także zapewniają sygnalizację hotelową i automatykę w pokoju. Zestaw funkcji automatyki jest bardzo duży i zawiera m.in. sterowanie klimatyzacją w systemie dwu- i czterorurowym, kontrolę dostępu do minibaru, zaawansowane metody sterowania zasilaniem elektrycznym oraz oświetleniem, detekcję otwarcia okna, różne sygnalizacje alarmowe, a także wykorzystanie pokoju w trybach z gościem zameldowanym i wymeldowanym. Kontrolery HRC mogą być wykorzystane do kontroli dostępu zarówno do pokoi, jak i do pomieszczeń wspólnych. Firma ROGER nie oferuje oprogramowania zarządzającego tymi kontrolerami i ogranicza się do udostępnienia protokołów komunikacyjnych umożliwiających ich konfigurację i zarządzanie. W tym przypadku oprogramowanie zarządzające zostaje dostarczone przez integratora, którym zwykle jest dostawca oprogramowania służącego do obsługi hotelu. Kompleksową usługę polegającą na dostawie oprogramowania do zarządzania hotelem i obsłudze urządzeń do kontroli dostępu i automatyki pokojowej od wielu lat ma w ofercie partner firmy ROGER – firma GiP, która specjalizuje się w oferowaniu systemów kontroli dostępu, automatyki i rozwiązań informatycznych przeznaczonych do zastosowania w obiektach hotelowych i pokrewnych w szeroko rozumianym sektorze HoReCa.

Podsumowanie

Ze względu na to, że liczba obiektów hotelowych w Polsce jest na razie o wiele mniejsza niż w krajach Europy Zachodniej, należy spodziewać się, że wraz z jej wzrostem nastąpi zwiększenie się zapotrzebowania na elektronikę budynkową. W związku z tym inżynierowie firmy ROGER pracują nad kolejnymi produktami, które mogą znaleźć zastosowanie w hotelach. Firma planuje dodać wkrótce do swojego asortymentu zamki mechatroniczne dostosowane do apartamentów przeznaczonych na wynajem krótkoterminowy, a także rozszerzyć swoją ofertę związaną z zarządzaniem zaawansowanymi systemami kontroli dostępu i automatyki przeznaczonymi do zastosowania w hotelach.

Grzegorz Wensker
ROGER

Postęp w dziedzinie kontroli dostępu
dzięki systemom otwartym

Axis Communications Poland

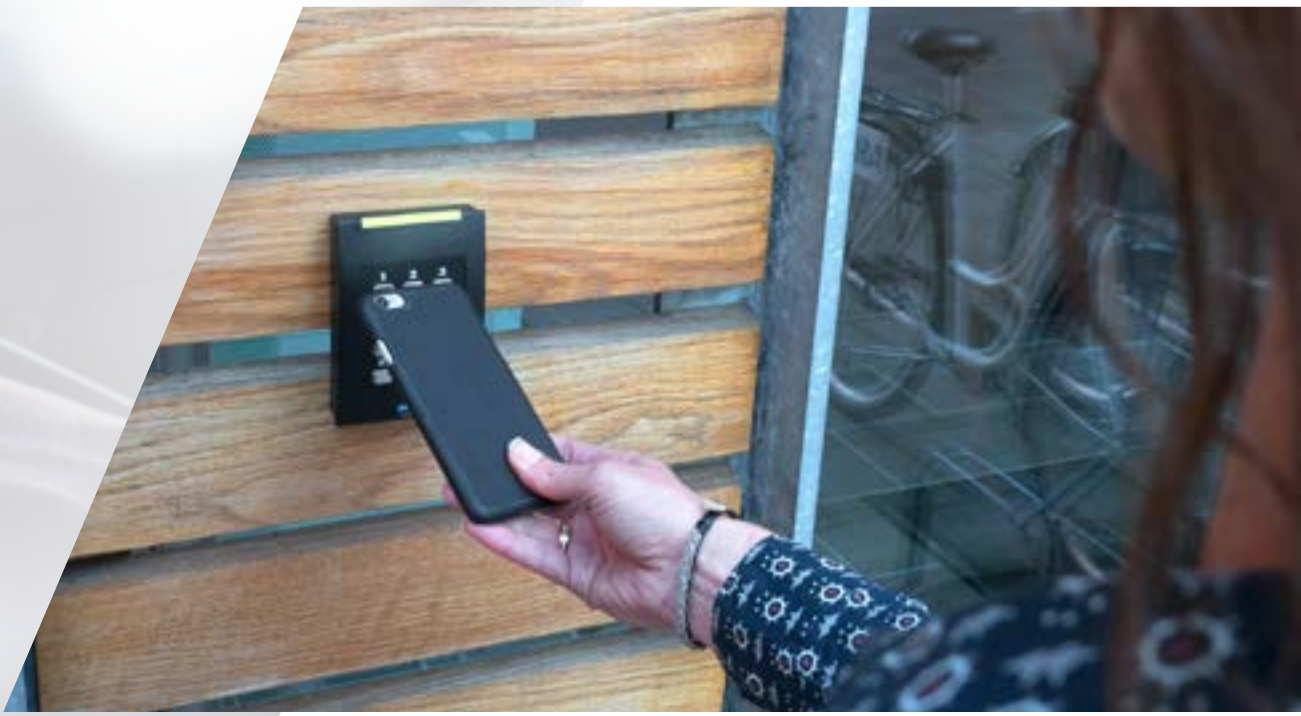
Najnowsze dane pokazują, że rok 2017 był drugim rokiem z rzędu, w którym systemy kontroli dostępu były najszybciej rozwijającym się sektorem w globalnej branży zabezpieczeń, stanowiącym obecnie 24% całego rynku. Wzrostową tendencję, która utrzymała się w roku 2018, przypisano zastąpieniu tradycyjnych firmowych rozwiązań (zamkniętych systemów) otwartymi platformami sieciowymi, co zwiększyło możliwości sprzętowe oraz poprawiło zarządzanie

Kontrola dostępu bazuje na stosunkowo prostej koncepcji – wejście lub wjazd danej osoby na chroniony teren jest możliwe, jeśli jest ona do tego uprawniona i uprawnienie to zostanie stwierdzone. Stosuje się ją na całym świecie, w różnych miejscach. Można powiedzieć, że w ostatnim czasie mamy do czynienia wręcz z rewolucją – technika kontroli dostępu zmienia się na naszych oczach.

Wady tradycyjnej techniki kontroli dostępu

W tradycyjnym systemie kontroli dostępu urządzenie sterujące zamkiem drzwiowym jest kontrolowane przez dostosowane do konkretnego rozwiązania oprogramowanie administracyjne, które ma wyznaczone funkcje związane z bezpieczeństwem. Bardziej zaawansowane i droższe systemy mają dodatkowe funkcje, jednak to producenci narzucają ramy ich funkcjonalności i możliwości ich składników – od kontrolerów i urządzeń uwierzytelniających po oprogramowanie. Z jednej strony stanowi to gwarancję działania systemu, lecz z drugiej ma skutek uboczny w postaci braku elastyczności, który wprawdzie może odpowiadać części dostawców, ponieważ narzuca nabywcy konieczność zakupu kompletnego systemu kontroli dostępu od jednego producenta, ale dla użytkownika końcowego jest rozwiązaniem skostniałym, uniemożliwiającym ewentualne wprowadzenie zmian.

Brak elastyczności, którym charakteryzuje się system zamknięty, może zniechęcać użytkowników końcowych – w razie potrzeby uzyskania nowych funkcji trzeba zastosować nowy system kontroli dostępu i całkowicie zdemontować poprzedni, co naraża dostawcę nie tylko na koszty, ale również na niedogodności organizacyjne i stratę czasu. Procedura zwykle powtarza się wraz z kolejnymi zmianami wymagań.

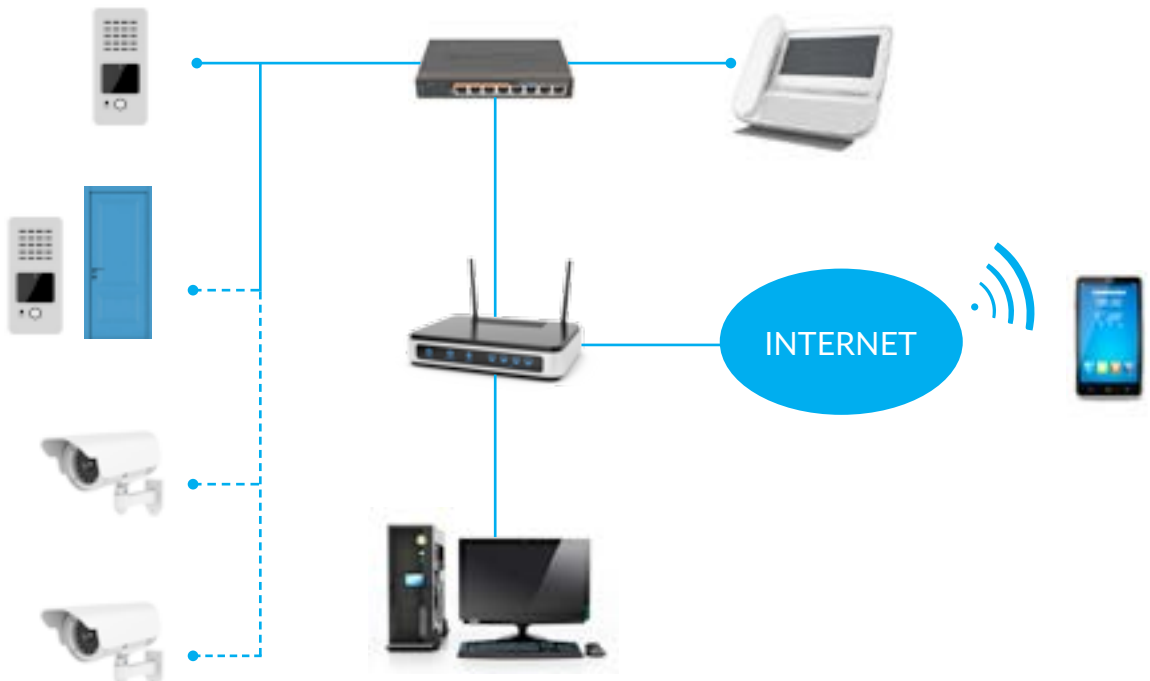


Zalety wykorzystania Internetu

Wykorzystanie protokołu IP oraz Internetu rzeczy daje nowe możliwości. Na przykład kamera jest w stanie stwierdzić, że osoba stojąca przy drzwiach i żądająca dostępu do chronionego obszaru nie jest prawowitym posiadaczem karty identyfikacyjnej, i automatycznie wygenerować ostrzeżenie oraz zablokować dostęp. Integracja kamery z innymi systemami, takimi jak HR, pomaga potwierdzić, że osoba usiłująca wejść to intruz. Może na przykład zostać wykryta próba posłużenia się kartą identyfikacyjną osoby przebywającej aktualnie na urlopie.

Przyszłość kontroli dostępu to otwarte systemy sieciowe. Ich możliwości są właściwie nieograniczone pod warunkiem zastosowania Internetu rzeczy (w odróżnieniu od tradycyjnej kontroli dostępu). Skalowalność i elastyczność systemów sieciowych pozwala użytkownikowi końcowemu wybrać na początek takie rozwiązanie, jakiego potrzebuje, a w miarę zmieniających się potrzeb rozbudować użytkowany system. Jest to rozwiązanie na teraz i na przyszłość.

Systemy kontroli dostępu Axis Communications wykorzystują otwarte protokoły. Dzięki temu można je dowolnie łączyć z najlepszym sprzętem i oprogramowaniem dostępnym na rynku oraz integrować z innymi systemami – także z używanym do tej pory systemem dozoru wizyjnego. Można je wykorzystywać do różnych celów – od podstawowej identyfikacji, przez kontrolę dostępu, aż po zaawansowane zarządzanie dostępem.



Otwartość oznacza, że można wybrać dowolne bazujące na otwartym standardzie elementy od dowolnego dostawcy i że możliwa jest integracja z oprogramowaniem i systemami innych producentów.

Axis Communications umożliwia także wykorzystanie kodów QR zamiast tradycyjnych plastikowych kart do potwierdzania tożsamości. Oferuje wiele różnych rozwiązań. Rozwiązania te nie tylko zmniejszają koszty zakupu, obsługi, drukowania, dystrybucji i utylizacji kart fizycznych, ale także mają bardzo pozytywny wpływ na środowisko i przyczyniają się do ograniczenia emisji dwutlenku węgla. Zastąpienie uwierzytelniania fizycznego cyfrowym jest kolejnym przykładem tego, jak Axis Communications dba o zrównoważony rozwój i dematerializację w systemach bezpieczeństwa i kontroli dostępu.

Rozwiązanie, w którym wykorzystuje się kody QR i urządzenia Axis Communications, jest udostępnione tylko za pośrednictwem naszych partnerów. W rozwiązaniu tym stosowana jest analiza obrazu kodu QR w kamerach sieciowych lub wideodomofonach w połączeniu z działaniem sieciowego kontrolera drzwiowego AXIS A1001, który komunikuje się z oprogramowaniem do kontroli dostępu innych producentów.

Wprawdzie kody QR nie są stosowane w systemach, które mają zapewnić wysoki stopień zabezpieczenia, jednak mogą przyczynić się do poprawy skuteczności zarządzania gośćmi w ogólnodostępnych obszarach budynku lub obiektu. Przykładem takiego zastosowania może być zarządzanie opóźnionymi dostawami, gdy na miejscu nie ma już personelu sklepowego, a także umożliwianie gościom hotelowym dostępu do parkingu lub do obiektu hotelowego poza godzinami pracy recepcji.

Gdy system kontroli dostępu współpracuje z wizyjnym systemem dozorowym firmy Axis Communications, lokalna kamera sieciowa marki Axis jest w stanie przesłać odczytany kod QR. W związku z tym nie są potrzebne czytniki kodów QR, których funkcję przejmują wszechstronne kamery sieciowe.

Axis Communications Poland

NOVUS®

NIEZAWODNE PRZEŁĄCZNIKI – ZASILANIE PoE DO 250 m

NAJLEPSZE ROZWIĄZANIA W ZAAWANSOWANYCH SYSTEMACH IP DUŻY BUDŻET MOCY DO 370 W

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Deklaracja EPD
firmy SALTO Systems

SALTO Systems

EPD [Environmental Product Declaration, czyli deklaracja dotycząca wpływu danego produktu na środowisko naturalne – przyp. red.] to niezależnie zweryfikowany dokument, w którym podaje się informacje o wpływie produktu na środowisko naturalne w całym okresie jego istnienia [„cyklu życia" – przyp. red.]. W tym przypadku dotyczy to zawężonej grupy produktów – inteligentnych elektronicznych zamków SALTO XS4 Original. Utworzenie EPD jest uznanym na całym świecie sposobem, dzięki któremu firmy mogą pokazać, tak jak SALTO Systems, że mają przejrzyste zasady odnoszące się do wpływu produkcji i konserwacji produktów na środowisko naturalne.

– *Utworzenie pierwszej deklaracji EPD dla modelu XS4 na etapie projektowania jest znaczącym osiągnięciem, z którego firma SALTO Systems powinna być bardzo dumna* – powiedział Aznar Sethna, dyrektor ds. marketingu i sprzedaży w SALTO Systems. – *Nie tylko wyznacza to punkt odniesienia dla branży kontroli dostępu, lecz także świadczy o rzeczywistym zaangażowaniu firmy SALTO w dbałość o zachowanie przejrzystych zasad postępowania mającego wpływ na środowisko naturalne i o poprawianie wyników tego postępowania.*

Modele SALTO XS4 i inteligentne zamki do kontroli dostępu firmy SALTO Systems, które można wykorzystać do modernizacji drzwi lub zastoso-

wać jako wyposażenie drzwi w nowych budynkach, zostały zaprojektowane tak, aby były przyjazne dla środowiska i przyczyniły się do osiągnięcia przez SALTO Systems tak dobrych wyników podanych w EPD. Przeprowadzanie analizy cyklu życia produktu przez firmy z branży technicznej i zajmujące się bezpieczeństwem nie należy do rzadkości. Weryfikacja EPD wymagała zgromadzenia danych i podania ich zgodnie z surowymi zasadami i normami.

– *Uzyskanie EPD dla całej rodziny produktów nie jest proste* – powiedział Ricardo Garcia, kierownik ds. jakości w SALTO Systems. – *Wymaga to zebrania i analizy znacznej ilości danych dotyczących całego okresu istnienia inteligentnego zamka – łącznie z określeniem jego wpływu na środowisko.*

– *Firma SALTO jest zaangażowana w tworzenie inteligentnych zamków z uwzględnieniem równowagi ekologicznej, więc te informacje przyczyniają się do dalszego doskonalenia naszych produktów* – powiedział Garcia. – *Dzięki określeniu wpływu naszych zamków na środowisko możemy zapewnić naszych partnerów i klientów, że przyszłe projekty będą jeszcze bardziej uwzględniać tę równowagę.*

Inteligentne, bezpieczne, innowacyjne oraz łatwe do zamontowania w drzwiach zestawy XS4 Original nie wymagają okablowania, są sterowane bezprzewodowo, zasilane bateryjnie, łączą się sieciowo i znajdują wiele zastosowań w kontroli dostępu. Wykorzystują najnowsze techniki identyfikacyjne i komunikacyjne (NFC i BLE) oraz umożliwiają dostęp bez użycia klucza.

Inteligentne zamki z serii XS4 Original zostały zaprojektowane tak, aby pasowały do większości standardowych drzwi i współdziałały z większością zamków wpuszczanych i zatrzaskowych zgodnych z normami europejskimi, skandynawskimi i ANSI. Są całkowicie zgodne z deklaracją EPD, przyczyniają się do oszczędzania zasobów naturalnych i mają ograniczony wpływ na środowisko. Inteligentne zamki i procesy technologiczne firmy SALTO Systems są w stanie sprostać najwyższym wymaganiom dotyczącym ochrony środowiska i oszczędzania zasobów.

SALTO Systems jest członkiem Institut Bauen und Umwelt e.V.

Jako członek Institut Bauen und Umwelt e.V. SALTO Systems pomaga stowarzyszeniu w osiąganiu jego celów – w szczególności w promowaniu zrównoważonego budownictwa. Aby osiągnąć ten cel, IBU prowadzi program deklaracji EPD typu III według norm ISO 14025 i EN 15804. Poprzez tworzenie deklaracji EPD i ich publikację w programie deklaracji IBU firma SALTO Systems podaje do publicznej wiadomości wszystkie istotne informacje o wpływie swoich produktów na środowisko naturalne. Dane zawarte w EPD bazują na analizie cyklu życia produktu i zostały zweryfikowane przez niezależnych audytorów.

Deklaracje EPD nie zawierają ocen wpływu produktów na środowisko naturalne. Służą raczej jako wiarygodne i niezależnie skontrolowane źródła informacji dla ekspertów z różnych dziedzin, w tym architektów, planistów, inżynierów i audytorów. W kontekście zintegrowanego planowania umożliwiają świadome podejmowanie decyzji i dokonywanie ocen, np. podczas wyboru produktu i certyfikacji budynku.

Więcej informacji o IBU i programie EPD znajduje się na stronie http://www.ibu-epd.com.

SALTO Systems
Tłumaczenie: Paweł Karczmarzyk

Bosch Building Technologies wprowadza Access Management System 2.0

Bosch Security and Safety Systems

Obecnie klienci oczekują systemów służących do zarządzania kontrolą dostępu, które są proste w obsłudze i konfiguracji. Muszą też być skalowalne adekwatnie do potrzeb oraz łatwe do zintegrowania z innymi rodzajami zabezpieczeń, takimi jak systemy dozoru wizyjnego czy systemy sygnalizacji włamania i napadu. Ponadto systemy do zarządzania kontrolą dostępu muszą być w wysokim stopniu stabilne i niezawodne. Wprowadzony przez firmę Bosch Access Management System (AMS) 2.0 spełnia wszystkie te wymagania

Fot. 1. Źródło: Bosch Security and Safety Systems

Określ swoje potrzeby, skonfiguruj i korzystaj

System został zaprojektowany w taki sposób, aby był dla klienta jak najprostszy w konfiguracji i obsłudze. Oprogramowanie jest oferowane w trzech wstępnie skonfigurowanych pakietach: Lite (maks. 144 drzwi i 200 000 posiadaczy kart), Plus (maks. 512 drzwi i 200 000 posiadaczy kart) oraz Professional (maks. 10 000 drzwi i 200 000 posiadaczy kart).

Konfiguracja nie jest skomplikowana. Istniejące mapy pięter można zaimportować do systemu, a następnie rozmieścić ikony reprezentujące kontrolery, drzwi i obiekty budowlane. Dodawanie użytkowników jest bardzo proste. Na przykład rejestracji i przydzielenia profili dostępu można dokonać w jednym oknie dialogowym.

Obsługa systemu również jest łatwa. Graficzny interfejs użytkownika jest przejrzysty i zrozumiały. Ciemna paleta kolorów interfejsu redukuje zmęczenie oczu, dzięki czemu operatorzy mogą łatwiej skoncentrować się na pracy, długo zachowując czujność. Kolorystyka interfejsu graficznego oprogramowania AMS współgra z kolorystyką interfejsu graficznego systemu BVMS (Bosch Video Management System), dzięki czemu obsługa jest łatwiejsza niż w przypadku dwóch odmiennych systemów.

Przyszłościowe rozwiązanie dzięki wysokiej skalowalności

Użytkownicy mogą zacząć od niewielkiego systemu, a potem go rozbudowywać, jeśli zajdzie taka potrzeba. Oprogramowanie AMS 2.0 można dostosować, gdyż obsługuje maksymalnie 10 000 drzwi i 200 000 posiadaczy kart identyfikacyjnych. Rozbudowa nie wymaga wymiany sprzętu. Użytkownicy muszą jedynie zainstalować rozszerzoną wersję oprogramowania i dodać kolejne kontrolery, czytniki i karty identyfikacyjne. Powiększenie rozmiarów systemu jest zatem nie tylko łatwe, ale także ekonomiczne, a ponieważ oprogramowanie jest regularnie aktualizowane i uzupełniane o dodatkowe opcje z zakresu bezpieczeństwa danych, stanowi także bezpieczną inwestycję. AMS 2.0 to rozwiązanie dostosowane do budynków administracji rządowej, placówek handlowych, dla instytucji oświatowych i wielu innych podmiotów.

Pełna dostępność i wysoka stabilność

W celu zagwarantowania maksymalnej stabilności i dostępności oprogramowanie AMS 2.0 zawiera Master Access Controller (MAC) jako dodatkowy bufor bezpieczeństwa pomiędzy serwerem a kontrolerami dostępu. W razie awarii serwera w AMS 2.0 jego zadania przejmuje MAC, zapewniając nieprzerwaną komunikację kontrolerów między sobą oraz udostępnianie niezbędnych informacji z czytników kart. Umożliwia to dalszą, nieprzerwaną obsługę takich funkcji jak *Anti-Passback* i *Guard Tour* realizowanych z użyciem różnych kontrolerów.

Funkcja *Anti-Passback* uniemożliwia posiadaczowi karty przekazanie jej innej osobie w celu umożliwienia nieautoryzowanego dostępu. *Guard Tour* to funkcja dla strażników, którzy na ustalonej trasie obchodu używają jako punktów kontrolnych czytników kart, przy których muszą być w określonym czasie. Każde odstępstwo od ustalonej kolejności lub przewidzianego czasu włącza alarm w systemie AMS. Umożliwia to szybkie powiadomienie osób odbierających zgłoszenia o zagrożeniu, co poprawia bezpieczeństwo pracy personelu zajmującego się ochroną.

W niezwykle rzadkich przypadkach awarii serwera AMS oraz systemu MAC posiadacze kart identyfikacyjnych nadal mogą wchodzić do stref i wychodzić z nich, korzystając ze swoich identyfikatorów, ponieważ baza danych znajduje się w kontrolerach AMC (Access Management Controllers). Dzięki możliwości pracy offline można uniknąć niebezpiecznych zdarzeń nawet podczas awarii systemu.

Wysoki standard bezpieczeństwa dzięki zarządzaniu poziomami zagrożenia

W systemie można zdefiniować maksymalnie 15 poziomów zagrożenia i określić, z czym mają

Fot. 2. Wizualizacja obiektu w oprogramowaniu Access Management System 2.0 (źródło: Bosch Security and Safety Systems)

być powiązane (tzn. z blokadą, kontrolowaną blokadą lub ewakuacją), co oznacza możliwość szybkiego zastosowania środków bezpieczeństwa w sytuacjach krytycznych, na przykład w razie pożaru lub ataku terrorystycznego. Określony poziom zagrożenia jest wskazywany na trzy sposoby – z użyciem stacji roboczej operatora, przycisku alarmowego lub przez przyłożenie do czytnika specjalnie skonfigurowanej karty alarmowej. Różne poziomy zagrożenia mogą spowodować różne reakcje, takie jak otwarcie wszystkich drzwi, zablokowanie wszystkich drzwi lub – w trybie mieszanym – otwarcie niektórych i zablokowanie pozostałych drzwi. Poszczególne drzwi mogą mieć przypisane indywidualne profile bezpieczeństwa i zapewniać dostęp tylko wybranym posiadaczom kart.

Wysoki poziom zabezpieczenia danych i ochrona prywatności

W celu ochrony przed cyberprzestępczością i utratą danych osobowych zarówno baza danych, jak i komunikacja pomiędzy serwerem i kontrolerami dostępu jest szyfrowana na wszystkich etapach, na przykład poprzez użycie bezpiecznego protokołu OSDP (Open Supervised Device Protocol) v2. Oprogramowanie AMS 2.0 stosuje także zaufane certyfikaty cyfrowe do wzajemnego uwierzytelniania komunikacji pomiędzy serwerem a klientem w celu zapobiegania manipulacjom ze strony nieuprawnionych klientów, a także zasady bezpiecznego projektowania, takie jak *secure-by-default* czy zasada „najmniejszego uprzywilejowania".

Rozwiązanie autonomiczne, przystosowane do integracji w ramach kompletnego systemu zabezpieczeń

AMS 2.0 to elastyczny system zarządzania kontrolą dostępu dla średnich i dużych podmiotów. Jest łatwy w konfiguracji, obsłudze i rozbudowie. Może być rozbudowywany, jeżeli zmienią się potrzeby użytkownika, i można go zintegrować z systemami dozoru wizyjnego, takimi jak BVMS (od wersji 9.0) oraz systemami innych producentów, np. Milestone XProtect. Od drugiego kwartału będzie można zintegrować go także z systemem sygnalizacji włamania i napadu serii B/G firmy Bosch oraz systemami innych producentów. Dzięki swoim możliwościom integracyjnym Access Management System może służyć jako solidna platforma umożliwiająca stosowanie różnych systemów zabezpieczeń w zależności od indywidualnych potrzeb użytkownika.

Opracowano na podstawie materiałów firmy Bosch Security and Safety Systems
Redakcja

EVIX®

MADE IN EU

NOWY WYMIAR OCHRONY
CZUJKI DUALNE PIR + MW

IDEALNE UZUPEŁNIENIE KAŻDEGO SYSTEMU ALARMOWEGO

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Kontrola dostępu a napowietrzanie

Kamil Więckowski

Dlaczego układy napowietrzające są tak ważne? Przede wszystkim umożliwiają prawidłowe działanie systemu oddymiania, którego zadaniem jest usunięcie dymu z drogi ewakuacyjnej. Bardzo często element wykonawczy układu napowietrzającego musi być zarazem elementem systemu kontroli dostępu, ewakuacyjnym i przeciwpożarowym. Najczęściej są to drzwi zewnętrzne, które muszą być odpowiednio zaryglowane i chronić przed włamaniem. Jak jest w przypadku, w którym drzwi służące do napowietrzania są dwuskrzydłowe? Na to i inne pytania można znaleźć odpowiedzi w niniejszym artykule

Cel stosowania układu napowietrzającego

Zadaniem układu napowietrzającego jest otwarcie drzwi napowietrzających po odebraniu sygnału sterującego z systemu oddymiania grawitacyjnego. Układ musi odryglować drzwi, a następnie je otworzyć. W przypadku drzwi dwuskrzydłowych otwarte muszą być kolejno skrzydła czynne i bierne. Cała operacja musi odbyć się w czasie nie dłuższym niż 60 s (zgodnie z wytycznymi normy EN-PN 12101-2 i rozporządzeniem 553 MSWiA z 27 kwietnia 2010 r.).

Cel stosowania systemu KD

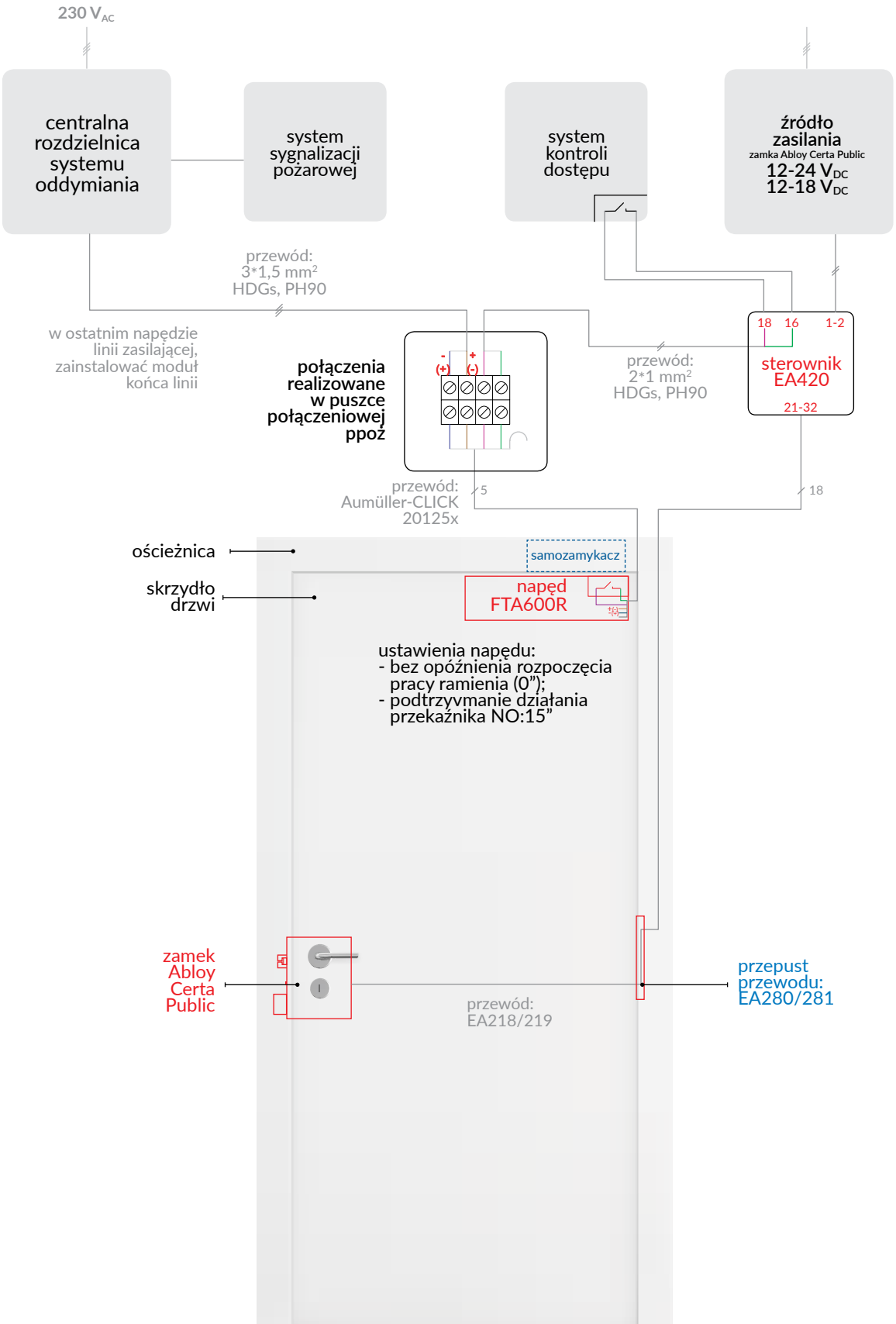
System kontroli dostępu umożliwia dostęp do obszarów chronionych tylko osobom uprawnionym i ograniczenie dostępu nieuprawnionych użytkowników do określonych stref. Każdy system składa się przynajmniej z dwóch rodzajów urządzeń. Pierwszy rodzaj to urządzenia wejściowe, które stwierdzają żądania wejścia do chronionych stref (szyfratory, czytniki kart, czytniki biometryczne), a drugi to elementy wykonawcze służące do zamykania i otwierania przejść (rygle elektromagnetyczne, zamki elektryczne, elektrozaczepy, szlabany). Za pomocą oprogramowania zarządzającego użytkownik systemu może w łatwy sposób nadawać uprawnienia poszczególnym osobom, a także je zmieniać.

Cel stosowania drzwi ewakuacyjnych

Zgodnie z PN-EN 179 oraz PE-EN 1125 drzwi muszą się otworzyć w efekcie pojedynczej czynności mechanicznej skutkującej oddziaływaniem określoną siłą, nawet gdy wcześniej były poddane naciskowi wstępnemu. Dodatkowo, ze względów bezpieczeństwa, powinny być zabezpieczone przed wejściem osób niepowołanych oraz przed próbą włamania. Aby uzyskać te wymagane i wskazane właściwości, można zastosować odpowiedni element ryglujący, np. zamek elektromotoryczny Abloy Certa Public, który będzie współpracował z napędem w systemie napowietrzającym wyposażonym w przekaźnik NO.

Fot. 1. ABLOY CERTA – zamki elektromotoryczne

Fot. 2. Zestaw zamka elektromotorycznego Abloy dla drzwi dwuskrzydłowych



Rys. 1. Sterowanie układem zamka Abloy i napędu napowietrzającego

Napowietrzanie

Zamki Abloy dobrze spełniają funkcję otwierania drzwi napowietrzających ze względu na automatyczne odryglowanie drzwi przed rozpoczęciem pracy siłowników oraz automatyczne zaryglowanie po zakończeniu napowietrzania. Zamki te rozwiązują często napotykany problem z drzwiami dwuskrzydłowymi, który polega na tym, że skrzydło bierne jest ryglowane w górnej i dolnej części drzwi, a podczas napowietrzania oba skrzydła muszą zostać odblokowane automatycznie. Otwarcie zamka Abloy Certa Public jest inicjowane poprzez styk bezpotencjałowy – zwarcie styków w sterowniku zamka EA420. Sygnał otwarcia może być wysyłany równolegle poprzez system kontroli dostępu i system oddymiania grawitacyjnego.

Odblokowanie górnego zamka skrzydła biernego jest inicjowane poprzez zasilenie cewki tego zamka. Po zainicjowaniu pracy napędów napęd skrzydła czynnego przesyła sygnał otwarcia do sterownika zamka Abloy Certa Public. Napęd skrzydła biernego zamyka obwód zasilający górnego zamka skrzydła biernego. Czasy działania wbudowanych przekaźników NO napędów, jakie należy ustawić, to 15 s dla skrzydła czynnego i 25 s dla skrzydła biernego. W przypadku drzwi jednoskrzydłowych współpraca podzespołów funkcjonalnych jest taka sama jak w przypadku skrzydła czynnego.

Kontrola dostępu

Systemy kontroli dostępu i klucze elektroniczne kontrolują jedynie uprawnienia dostępowe i wejścia jako zdarzenia w systemie bez użycia dodatkowych elementów monitorujących. Zamki elektromotoryczne dostarczają o wiele więcej informacji o stanie drzwi za pośrednictwem sygnałów monitorujących. Zamek samoczynnie przetwarza informacje z systemów zabezpieczeń i sygnały alarmowe oraz przekazuje informacje o stanie rygla (wysunięty, zasunięty), otwarciu drzwi, celowym uszkodzeniu kabla, użyciu klamki od strony ewakuacyjnej czy otwarciu drzwi za pomocą klucza. W kontroli dostępu głównym i istotnym parametrem jest wytrzymałość mechaniczna zamka. Dzięki temu, że po zamknięciu drzwi automatycznie się zatrzaskują (funkcja samoryglowania), wytrzymałość mechaniczna zamka sięga nawet 4000 kg. Często w przypadku zastosowania innych rozwiązań, takich jak zwory elektromagnetyczne czy elektrozaczepy, nie jest możliwe osiągnięcie nawet jednej dziesiątej tej wartości. Drzwi napowietrzające są często drzwiami zewnętrznymi, które powinny być solidnie zabezpieczone, co wynika chociażby z warunków ubezpieczenia. Drzwi antywłamaniowe mają być przede wszystkim solidnie ryglowane. Jeśli elementami ryglującymi są zwory lub elektrozaczepy nie jest możliwe spełnienie tego wymagania i jednoczesne zapewnienie automatycznego napowietrzania po otrzymaniu sygnału z systemu oddymiania.

Bezpieczeństwo

W wielu przypadkach drzwi muszą spełniać wiele wymagań jednocześnie. Pełnią one rolę drzwi przeciwpożarowych i ewakuacyjnych, a jednocześnie służą do napowietrzania. Zamki elektryczne Abloy zapewniają otwarcie mechaniczne za pomocą klamki bądź dźwigni antypanicznej. Działają we wszystkich okolicznościach, niezależnie od rodzaju systemu zarządzania czy napięcia zasilania. Spełniają wymagania norm ewakuacyjnych EN179 i EN1125 oraz przeciwpożarowej EN1634-1. Gwarantują bezproblemowe wyjście w przypadku zagrożenia, więc można w nie wyposażyć drzwi ewakuacyjne i jednocześnie przeciwpożarowe.

Kamil Więckowski
ASSA ABLOY Poland

blueSmart
w głównej siedzibie firmy NORD Napędy

Winkhaus Polska

NORD Napędy to polski oddział Getriebebau NORD – jednego z czołowych producentów mechanizmów napędowych. Niezawodne reduktory, przekładnie, silniki oraz elektronika napędowa tej firmy są wykorzystywane na całym świecie, zarówno w obiektach przemysłowych, w dźwigach portowych, jak i na stadionach czy w teatrach. Hasło „Napędy NORD poruszają rzeczy na całym świecie" oddaje istotę działalności firmy

Wybranie produktów Winkhaus przez tak znaczącą firmę jak NORD Napędy bardzo nas cieszy i utwierdza w przekonaniu, że elektroniczny system dostępowy blueSmart to idealne rozwiązanie dla przedsiębiorstw. Dlaczego? Centralne zarządzanie uprawnieniami do dostępu do poszczególnych pomieszczeń, możliwość integracji z systemami służącymi do rejestracji czasu pracy i kontroli dostępu do chronionych stref budynku, a także wygoda będąca rezultatem zamiany pęku kluczy na jeden poręczny identyfikator to tylko kilka najważniejszych powodów.

Zgubienie klucza to już nie problem

W przeciwieństwie do systemów z wkładkami mechanicznymi i kluczem centralnym w blueSmart wykorzystywane są wkładki elektroniczne. Wszelkie zmiany organizacyjne, obejmujące także dezaktywację zgubionych kluczy, są wprowadzane do systemu dosłownie kilkoma wciśnięciami klawiszy klawiatury komputera centralnego. Dzięki elastyczności systemu blueSmart zgubienie klucza nie skutkuje koniecznością kosztownej i pracochłonnej wymiany wkładek. Nie trzeba ręcznie programować wkładek w poszczególnych drzwiach.

Fot. 1. Główna siedziba firmy NORD Napędy w Zakrzowie

Fot. 2. Hala serwisowa firmy NORD Napędy w Zakrzowie

Aktualizacja uprawnień dostępowych jeszcze nigdy nie była tak prosta.

Dokładne raportowanie

Na potrzeby firmy NORD Napędy klucze blueSmart zostały wyposażone w dodatkowy transponder, który umożliwia bezprzewodową identyfikację użytkownika również w innych używanych w firmie systemach RFID. Daje to między innymi możliwość wygodnego zarządzania czasem pracy oraz dostępem do stref chronionych za pomocą jednego identyfikatora. System blueSmart umożliwia również raportowanie obecności danej osoby w pomieszczeniu, a także uzyskanie informacji na temat prób użycia nieuprawnionego klucza.

Wygodna instalacja

Wkładki elektroniczne, które są ważnym elementem systemu blueSmart, nie wymagają żadnego okablowania. Dzięki temu, że mają wymiary standardowych wkładek patentowych, mogą być zamontowane w większości drzwi – zarówno nowych, jak i już użytkowanych. Wkładki są zasilane wydajnymi bateriami, których stan jest monitorowany w systemie centralnym.

Bezprzewodowa komunikacja

W systemie blueSmart klucze są jednocześnie nośnikami danych dostępowych. Aktualizacja danych odbywa się poprzez sieć bezprzewodową podczas kontaktu klucza z czytnikiem lub wkładką. W chwili, gdy pracownik przykłada swój klucz do czytnika lub wkłada go do elektronicznej wkładki, następuje wymiana danych, której skutkiem może być np. zmiana praw dostępu do pomieszczeń, aktualizacja czasowych ograniczeń dostępu czy uzyskanie informacji o stanie baterii. Całość jest administrowana za pomocą oprogramowania opracowanego przez Winkhaus. Jest ono wygodnym i sprawdzonym narzędziem do zarządzania systemami kontroli dostępu o różnym stopniu złożoności.

blueSmart w firmie NORD Napędy

System blueSmart zarządza dostępem w głównej siedzibie polskiego oddziału firmy NORD, która znajduje się w Zakrzowie. To tu pracownicy zajmują się obsługą klienta, doradztwem technicznym, serwisem oraz odbywają się szkolenia. W obiekcie składającym się z nowoczesnego biurowca o powierzchni 2000 m^2 z zapleczem szkoleniowo-konferencyjnym oraz centrum serwisowo-warsztatowym o powierzchni 700 m^2 zamontowano 60 wkładek elektronicznych i dwa czytniki aktualizujące uprawnienia dostępowe.

Fot. 3. Wkładka elektroniczna Winkhaus blueSmart z zewnętrzną baterią

– Z perspektywy czasu bardzo pozytywnie oceniam decyzję o zainstalowaniu systemu blueSmart w naszej firmie. Dzięki temu systemowi jesteśmy w stanie prosto, szybko i niskim kosztem zarządzać strefami dostępu dla każdej osoby. Stwarza to duże możliwości i pozwala w bardzo łatwy sposób organizować pracę naszym pracownikom – powiedział Jarosław Bilich, dyrektor zarządzający firmy NORD Napędy.

Winkhaus Polska

Podsumowanie działalności ONVIF w 2019 r.
podczas dorocznego spotkania członkowskiego

Andrea Gural

ONVIF, czołowa globalna organizacja normalizacyjna zajmująca się zabezpieczeniami fizycznymi opartymi na protokole IP, odbyła w listopadzie swoje doroczne spotkanie członkowskie. Na spotkaniu omówiono ważne działania w roku 2019 i cele na kolejny rok. Uczestnicy wysłuchali prelekcji na temat rozwoju ONVIF, a także planów dotyczących opracowania nowej specyfikacji ONVIF

Przewodniczący ONVIF, Per Björkdahl, podkreślił osiągnięcia tej organizacji w ciągu ostatniego roku, w szczególności utrzymywanie ciągłego kontaktu z producentami sprzętu. Pod koniec bieżącego roku liczba produktów zgodnych ze specyfikacją ONVIF przekroczyła 13 000. Dzięki możliwości wyboru między sześcioma profilami ONVIF i dodatkowym, siódmym, który jest w fazie rozwoju, profile te są coraz częściej włączane do różnych procesów przetargowych i specyfikacji projektowych na całym świecie. Björkdahl podkreślił również ciągłe zaangażowanie ONVIF w prace normalizacyjne Międzynarodowej Komisji Elektrotechnicznej mające na celu zapewnienie interoperacyjności między różnymi systemami.

Zarząd ONVIF docenił wkład wielu osób z różnych komitetów ONVIF w tworzenie nowych profili. Steve Wolf, który zasiadał w kilku komitetach w imieniu Pelco, otrzymał nagrodę ONVIF Service Award, która jest przyznawana osobom, które długoterminowo zaangażowały się w pracę w dla organizacji. Podczas pracy w Komitecie Technicznym Wolf kierował Grupą Roboczą ds. Bezpieczeństwa, a także był aktywnym uczestnikiem Grupy Roboczej ds. Ulepszania Systemów Wizyjnych i przyczynił się do wprowadzenia wielu poprawek w systemach tego typu.

Andreas Schneider z Sony otrzymał nagrodę ONVIF Distinguished Service Award, która wyróżnia osoby, które przez wiele lat miały znaczący wkład w działania ONVIF na wielu stanowiskach. Długoterminowe usługi Schneidera w Komitecie ds. Usług Technicznych sprawiły,

że jest on głównym koordynatorem organizacji ONVIF i przyczynił się do powstania wielu profili ONVIF.

– Nadrzędnym celem ONVIF jest wprowadzenie na rynek jednego interfejsu, za pomocą którego można obsłużyć każdy system – powiedział Björkdahl. *– Wyróżnieni przedstawiciele wykazali znaczące i długoterminowe zaangażowanie w prace naszej organizacji, co przybliżyło realizację tego celu. Dziękujemy obu wyróżnionym za innowacyjność, ciężką pracę i zaangażowanie.*

Przewodniczący Komitetu Technicznego ONVIF, Hans Busch z firmy Bosch, rozmawiał z członkami o planach dotyczących rozwoju specyfikacji

cję przewodniczącego Komitetu Komunikacyjnego ONVIF, przedstawił podsumowanie działań komunikacyjnych ONVIF w 2019 r. i omówił plany organizacji dotyczące uruchomienia chińskojęzycznej strony internetowej pod koniec tego roku.

Założona w 2008 r. organizacja ONVIF jest czołowym i uznanym forum branżowym mającym na celu zwiększenie interoperacyjności zabezpieczeń technicznych opartych na protokole IP. Organizacja ma globalną bazę członków uznanych firm z branży wizyjnych systemów zarządzania i kontroli dostępu oraz ponad 13 000 produktów zgodnych z profilami. Profil S dotyczy strumieniowego przesyłania obrazów z kamer, Profil G – rejestracji i przechowywania

ONVIF, tworzeniu nowych profili i kontynuacji prac w ramach grup roboczych IEC TC 79 – Grupy Roboczej ds. Wizyjnych Systemów Dozorowych i Grupy Roboczej ds. Systemów Kontroli Dostępu. Busch mówił zwłaszcza o tym, jakie specyfikacje są badane pod kątem przyszłych profili oraz w jaki sposób uzupełniają i dalej ulepszają istniejące profile ONVIF.

Andreas Schneider jako przewodniczący Komitetu ds. Usług Technicznych przedstawił przegląd prac komitetu nad nowymi i istniejącymi profilami, narzędziami do testowania stacji roboczych i urządzeń wchodzących w skład systemów, a także nad aktualizacjami dotyczącymi zgodności i narzędzi oraz organizacji spotkań roboczych dla programistów. Shi-lin Chan z Axis Communications, który pełni funk-

obrazów, Profil C – systemów kontroli dostępu, Profil Q – urządzeń gotowych do użycia od razu po wyjęciu z opakowania, Profil A – rozszerzonej konfiguracji systemów kontroli dostępu, a Profil T – zaawansowanego, strumieniowego przesyłania danych. ONVIF kontynuuje współpracę ze swoimi członkami w celu zwiększenia liczby rozwiązań interoperacyjnych, które są zapewniane przez produkty zgodne z ONVIF.

Więcej informacji na temat produktów zgodnych z ONVIF, w tym urządzeń dostarczanych przez firmy członkowskie, jest dostępnych na stronie internetowej www.onvif.org.

Bezpośr. inf. Andrea Gural
Eclipse Media Group
Tłumaczenie: Andrzej Walczyk

Bezpieczeństwo kontraktowe inteligentnych budynków

Piotr Kaniewski

Inteligentnych budynków przybywa. Za inteligentny budynek można uznać, w uproszczeniu, taki obiekt, który jest wyposażony w liczne czujki i czujniki oraz jest obsługiwany przez zespół zintegrowanych i centralnie zarządzanych systemów informatycznych (często wykorzystujących najnowsze zdobycze techniki, takie jak chmura obliczeniowa i sztuczna inteligencja)

Zainteresowani inwestowaniem w inteligentne budynki poświęcają coraz więcej uwagi kwestiom związanym z bezpieczeństwem obiektu, czyli z jego zabezpieczeniem przed cyberatakami. Niestety nie zawsze są świadomi ważności tzw. bezpieczeństwa kontraktowego.

Przez bezpieczeństwo kontraktowe inteligentnego budynku należy rozumieć taki stan dokumentacji kontraktowej dotyczącej urządzeń i systemów informatycznych zastosowanych w obiekcie, który daje instrumenty prawne wymuszające ciągłe, nieprzerwane, wydajne i bezpieczne korzystanie z nich, możliwość rozwoju, a także możliwość wpływania na dostawców takich urządzeń i systemów, a w ostateczności sprawnego zakończenia współpracy z nimi. Jest to kwestia tym istotniejsza, im więcej elementów IT jest zastosowanych w budynku i im bardziej są skomplikowane technicznie.

Co wpływa na bezpieczeństwo kontraktowe

Stworzenie i wynegocjowanie bezpiecznych i korzystnych umów zależy od wielu czynników. Jedne z nich będą w danym przypadku ważniejsze od innych, jednak zawsze należy zadbać o utrzymanie i dostępność urządzeń i systemów, możliwość audytowania, rozwój oprogramowania, prawa autorskie i odpowiedzialność dostawcy za przedmiot umowy.

Utrzymanie i dostępność urządzeń i systemów

Dobry system IT różni się od złego przede wszystkim tym, że jest dostępny i działa poprawnie, tzn. błędy występują niezbyt często (chociaż są nieuniknione) i można je szybko naprawić. Jest to podstawą tzw. umów utrzymaniowych. Odpowiednie określenie parametrów, czasów i procedur naprawy komponentów IT jest niezbędne w celu zapewnienia spokojnego użytkowania inteligentnych budynków. Ogromne znaczenie ma definiowanie błędów. Należy je zdefiniować w sposób jasno określający zakres odpowiedzialności dostawcy. Chodzi tu m.in. o zdefiniowanie luki w systemie, wycieku danych, podatności na ataki i udanego ataku.

Możliwość przeprowadzenia audytu

Każde rozwiązanie IT zastosowane w inteligentnym budynku powinno być możliwe do zaudytowania. Dotyczy to zarówno samej struktury informatycznej systemu, jak i postanowień kontraktu (które powinny przyznawać odpowiednio szerokie prawo do audytu). Ma to duże znaczenie ze względu na bezpieczeństwo, integrację z innymi systemami IT, zarządzanie inteligentnymi budynkami, a także ich nabywanie.

Rozwój oprogramowania

Oprogramowanie, w które wyposażony jest budynek, powinno umożliwiać jego rozwój. Wydaje się to oczywiste. Trudniejsze jest stworzenie odpowiednich mechanizmów kontraktowych, które zapewnią możliwość dokonywania uaktualnień, rozbudowywania lub zmieniania funkcji w taki sposób, aby dostawca IT nie doprowadził do uzależnienia od siebie właściciela czy zarządcy nieruchomości lub do narzucania mu cen.

Prawa autorskie

Z prawnego punktu widzenia systemy IT to ogromne zbiory utworów – chronionych (bardzo rygorystycznie) przez prawo autorskie. Inwestując w rozwiązania informatyczne, należy zapewnić sobie odpowiednie uprawnienie do ich eksploatacji – nabyć prawa autorskie lub uzyskać licencję. Do tego trzeba pamiętać o prawie do modyfikacji i prawach zależnych, prawach do dokumentacji i kodu źródłowego, integracji z innymi systemami, zagrożeniach związanych z otwartością kodu źródłowego, a także czasie obowiązywania licencji. Niedostateczne przywiązywanie wagi do własności intelektualnej może mieć dotkliwe konsekwencje. Może doprowadzić do niemożności integracji danych rozwiązań z innymi rozwiązaniami informatycznymi, konieczności poniesienia dodatkowych opłat, braku możliwości rozwoju czy uzależnienia się od konkretnego dostawcy.

Odpowiedzialność

W umowach należy zmotywować lub zdyscyplinować dostawcę rozwiązań informatycznych przeznaczonych do zastosowania w inteligentnych budynkach, gdyż utartą praktyką jest ograniczanie odpowiedzialności nawet do stu procent różnie określanego przedmiotu umowy. Takie ograniczenie jest akceptowalne, o ile przewidziane zostaną wyjątki – dotyczące m.in. poufności i bezpieczeństwa danych, cyberataków czy wad prawnych. Standardem na rynku IT jest także wyłączanie odpowiedzialności dostawcy za utracone korzyści zamawiającego. W branży nieruchomości może to być problematyczne. Nieprawidłowe funkcjonowanie systemu IT może przecież doprowadzić do niepowodzenia transakcji, której przedmiotem jest budynek, w którym zastosowano ten system, albo nawet do poważnego zakłócenia ciągłości działalności biznesowej użytkownika systemu IT (np. awaria systemu regulującego może doprowadzić do drastycznego i katastrofalnego w skutkach wzrostu temperatury w magazynie z żywnością). Warto zwrócić na to uwagę. Ponadto awarie systemów informatycznych w budynkach mogą mieć katastrofalne skutki wizerunkowe. Należy to uwzględnić podczas negocjacji z dostawcą dotyczących umowy.

Często zdarza się, że dostawca nie jest jego producentem. Wówczas należy jasno określić jego obowiązki oraz zapewnić sobie możliwość otrzymania pewnych świadczeń od producenta. Dobrą praktyką jest także pośredniczenie dostawcy w załatwianiu przez klienta spraw z producentem.

Opisane wyżej zagadnienia są nowością w przypadku rynku nieruchomości, za to standardem w innych branżach, które wcześniej przeszły tzw. cyfryzację. Najważniejsze dla właścicieli i operatorów inteligentnych budynków jest poznanie zagadnień prawno-kontraktowych i uzyskanie fachowego doradztwa przy projektowaniu i negocjowaniu umów dotyczących rozwiązań informatycznych.

Piotr Kaniewski
e-mail: Piotr.Kaniewski@ssw.solutions
tel. kom.: +48 785 469 797

Instytut Bezpieczeństwa Pożarowego

NODEX

www.IBPNODEX.pl

Niezależny Ośrodek Doradców i Ekspertów

- Organizujemy zaawansowane kursy specjalistyczne i szkolenia dedykowane z zakresu bezpieczeństwa pożarowego
- Kładziemy duży nacisk na ćwiczenia i zajęcia laboratoryjne
- Współpracuje z nami ponad trzydziestu wykładowców i specjalistów

Atrakcyjne zniżki dla Członków Wspierających Rozwój Instytutu!

- Posiadamy doskonale wyposażoną salę szkoleniową z własną komorą testową
- Wykonujemy ekspertyzy oraz opinie dotyczące zabezpieczeń przeciwpożarowych i ewakuacji
- Zajmujemy się doradztwem technicznym dla inwestorów, wykonawców i projektantów.

Instytut Bezpieczeństwa Pożarowego NODEX Sp. z o.o.
ul. Pola Karolińskie 4, 02-401 Warszawa
tel.: +48 22 203 59 21, fax: +48 22 203 58 31

www.IBPNODEX.pl

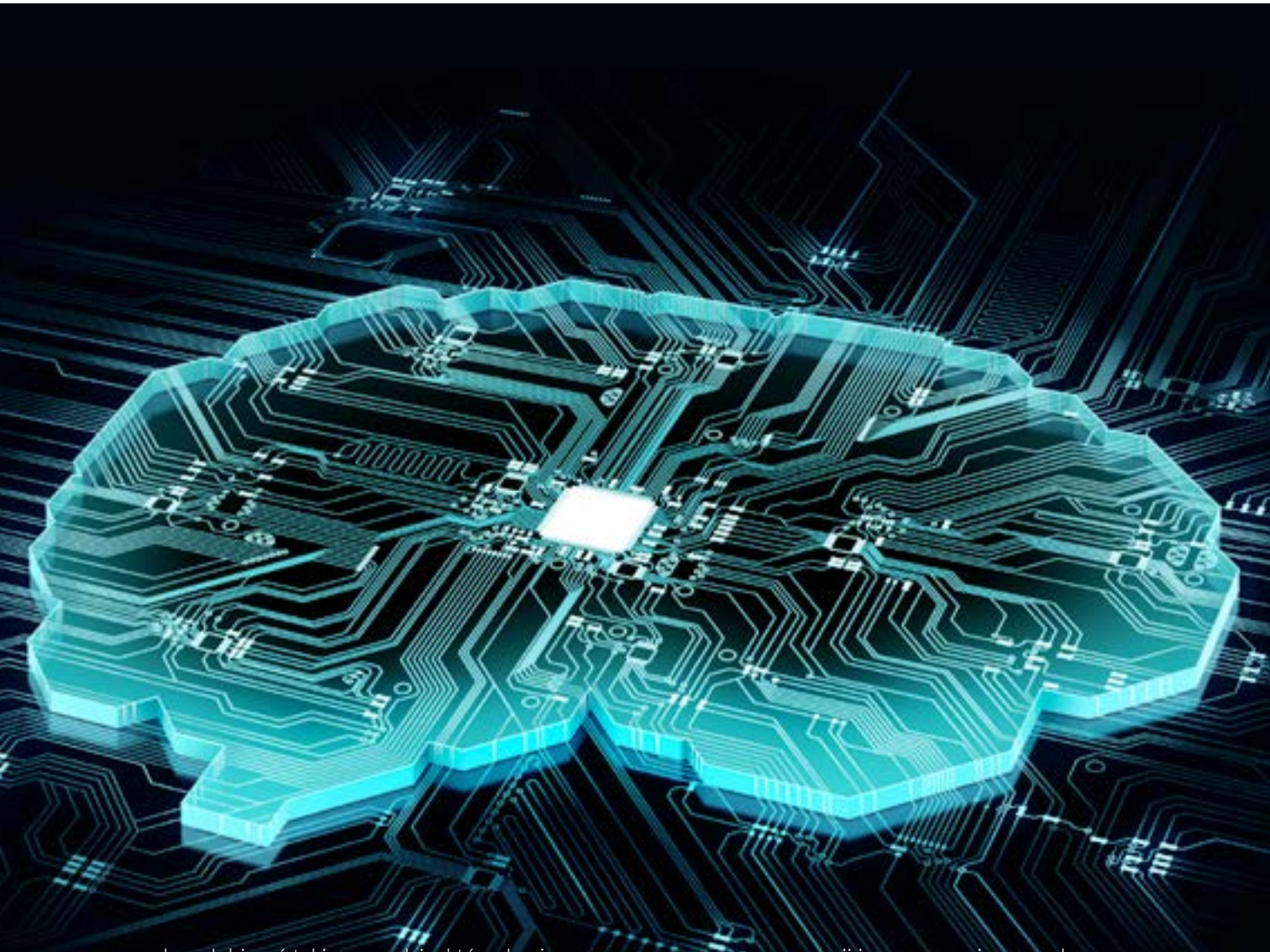
Kronos Alicja
krzemowy intelekt

mgr inż. Bartłomiej Dryja

Z zaciekawieniem obserwuję, jak postęp w dziedzinie techniki wypływa na zmiany w społeczeństwie. Nasi przodkowie wynaleźli druk, dzięki czemu dostęp do wiedzy stał się powszechny. Pradziadowie dokonali rewolucji w przemyśle i transporcie dzięki wykorzystaniu pary. Ojcowie zaczęli wykorzystywać na wielką skalę elektryczność i światło elektryczne, co spowodowało zmianę odwiecznego cyklu dobowej aktywności człowieka i tym samym dało premię w postaci czasu na własny rozwój po dniu ciężkiej pracy. My zaś mamy rewolucję cyfrową i automatyzację – proste czynności przejmują automaty i sieci neuronowe, a my przenosimy się w świat Internetu, smartfonów i chmur. Zmiany te docierają także do branży ochrony, a nawet do tak wąskiej dziedziny jak oprogramowanie CMS do zarządzania stacją monitorowania

Można powiedzieć, że wręcz narzuca nam się korzystanie z chmur, które stworzono, aby umożliwić jak najlepszy i jak najszybszy dostęp do bogatych zasobów informacji niezależnie od miejsca pobytu oraz wprowadzić płynną skalowalność mocy obliczeniowej. Czy jednak właśnie tego potrzebujemy w przypadku stacji monitorowania, w której w miarę stałe zasoby są potrzebne całodobowo, a mobilność na co dzień nie jest wymagana? Rezygnujemy z prywatności i wprowadzamy do sieci informacje o szczególnym znaczeniu, które nigdy nie powinny tam trafić. Czy na pewno wiemy, kto z tych informacji korzysta? Nie chodzi tu o złą wolę dostarczyciela usługi monitorowania, ale o zmiany prawa w Chinach i USA, które zmuszają właścicieli chmur do udostępniania danych na żądanie agencji rządowych. Nie możemy zapomnieć też o zmianach w planie zarządzania bezpieczeństwem, aby uwzględnić kilka dodatkowych elementów, które są poza naszą kontrolą. Mowa tu o infrastrukturze Internetu, serwerach wspomagających, takich jak DNS, dostawcach usług chmurowych i wreszcie o dostarczycielach samych usług monitorowania. Zeszłoroczne problemy Google, Amazona i Microsoftu dowiodły, że chmury mogą przestać działać, a nasz wpływ na to jest żaden. A co z kumulacją ryzyka? Atak na serwer w Internecie ma swoją konkretną cenę w Darknecie. Aby chmura mogła być tania, kilku odbiorców musi być obsługiwanych za pomocą jednej maszyny. Mamy więc sytuację, w której wyłączenie usługi na skutek ataku DoS na jedną agencję ochrony wyłącza pozostałe. Korzystając z chmury, musimy zaakceptować ograniczenia wynikające z użycia przeglądarki. Swoją drogą, czy ktoś pomyślał, jaką moc obliczeniową i ile energii marnujemy w skali świata, gdyż nie wykorzystujemy mocy naszych komputerów z procesorami i3, i5 lub nawet i7, ponieważ uruchamiamy na nich program, który wyświetla tylko dane przetwarzane gdzieś indziej? Chyba umknęła nam idea przetwarzania rozproszonego z początków rewolucji cyfrowej na początku lat 70., gdy duże maszyny były zastępowane setkami małych, pracujących w domach.

Czy powinniśmy bać się postępu w dziedzinie techniki? Oczywiście, że nie. Musimy jednak



mądrze dobierać takie narzędzia, których użycie ma sens, i stosować je do celów, do których powstały. Czy coś z tych wszystkich idei, które są nam znane z innych branż, znajduje zastosowanie w ochronie? Oczywiście, że tak. Przykładem jest Kronos Alicja oferowana przez firmę NEXT!. Alicja to zestaw sieci neuronowych i usług, które mają wspomóc dyspozytora, a w przyszłości będzie mogła całkowicie go zastąpić. Alicja jest ciągle rozwijana i na razie jest prototypem, jednak już teraz dużo potrafi. Może samodzielnie przeprowadzić wideoobchód, rozpoznać osoby, pojazdy, przedmioty i zwierzęta, może do kogoś zadzwonić i poinformować o alarmie, a także wysłać grupę interwencyjną. Wkrótce będzie umiała więcej, gdyż pilnie ją uczymy. Nie mamy wątpliwości, że to właściwa ścieżka rozwoju programów CMS, gdyż rozwiązuje podstawowy problem, który istnieje od samego początku stosowania programów do monitorowania, a mianowicie problem dostępności najcenniejszego zasobu, jakim jest człowiek. Czas, jakim dysponuje operator, jest ograniczony, tak jak liczba zagadnień, którymi może się zająć w danej chwili. Pomimo ciągłej poprawy ergonomii i uproszczenia procedur nadal na jednego operatora może przypadać od kilkuset do kilku tysięcy obiektów chronionych. Wszystko zależy oczywiście od rodzaju świadczonej usługi. A gdyby na dyspozytora mogło przypadać nie kilka tysięcy, lecz dziesięć tysięcy, dwadzieścia tysięcy, a może nawet więcej obiektów i gdyby człowiek tylko wspierał i nadzorował pracę sieci neuronowych i automatów? Pomyślcie, jakie dałoby to oszczędności. Jeśli weźmie się pod uwagę, że sieć neuronowa nie choruje, nie bierze urlopu, nie ma gorszych i lepszych dni oraz nigdy nie bywa zmęczona, to łatwo sobie wyobrazić, jaki skok jakościowy jest możliwy.

Jesteśmy przekonani, że rozwój systemu Kronos Alicja to właściwy kierunek, który zmieni całą branżę monitorowania, a lata doświadczenia zdobytego przez nas zespół przy kilkuset wdrożeniach aplikacji Kronos NET na całym świecie (od 2002 roku) to gwarancja powodzenia prac.

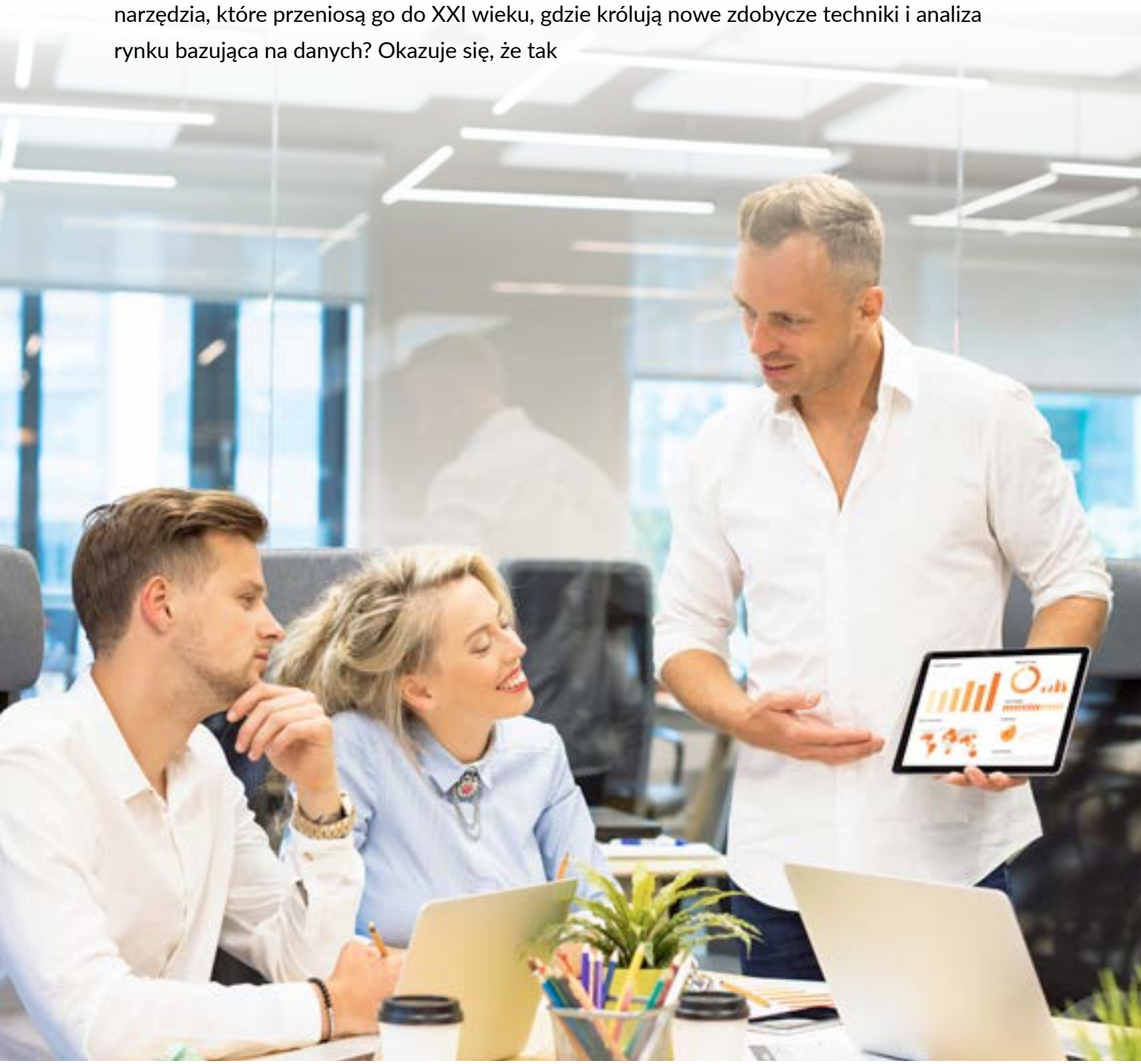
mgr inż. Bartłomiej Dryja
NEXT!

Sprzedaż usług ochrony

Wykorzystanie nowych narzędzi warunkiem przetrwania

Dariusz Nawojczyk

Świat pędzi, jak oszalały, ale jedna rzecz pozostaje niezmienna – sposób sprzedaży bezpośredniej. Niemal każda branża, w tym branża usług ochrony, od wielu lat kultywuje ten sam model. Główną rolę odgrywa osamotniony doradca z dobrą prezencją, broszurą reklamową i długopisem w ręku. Czy można coś zmienić? Czy sprzedawca może dostać narzędzia, które przeniosą go do XXI wieku, gdzie królują nowe zdobycze techniki i analiza rynku bazująca na danych? Okazuje się, że tak



Ciągle w tym samym miejscu

Czasem wydaje się, że o narzędziach sprzedażowych powiedziano już wszystko. Sprzedawca bierze ze sobą teczkę z materiałami, spotyka się z klientem, a później robi notatkę w CRM. Jego przełożony sprawdza notatkę i na jej podstawie podejmuje określone decyzje. Czy to wystarcza?

Po pierwsze – od sprzedawcy wymaga się ciągłego wzrostu rocznej sprzedaży, ale nie daje mu się nowych narzędzi pracy. Nadal ma do dyspozycji przede wszystkim swoje usta i ręce oraz komplet materiałów drukowanych (folderów, ulotek z informacjami dotyczącymi produktów etc.). To bardzo ogranicza jego możliwości. Sprzedawcy, którzy chcą sprostać wymaganiom, muszą pracować po dziesięć godzin dziennie lub więcej. Nie mają ze sobą czegoś, co dałoby im realną przewagę nad konkurencją w kontakcie z coraz bardziej wymagającymi i trudnymi klientami.

Po drugie, uzupełnianie CRM *post factum* daje słabe rezultaty, ponieważ dane zbierane w ten sposób są deklaratywne – ich jakość zależy w całości od sprzedawcy. Sprytny handlowiec wpisze do CRM dokładnie to, czego spodziewa się organizacja. Firma nie zdobywa w ten sposób informacji, dzięki którym może podjąć decyzje zarządcze.

Wymagania klientów rosną

Badanie przeprowadzone przez firmę Salesforce pt. *State of the Connected Customer 2018* pokazuje, że aż 80% klientów potwierdza rolę ich wrażeń z procesu sprzedaży, które stawiają na równi z samym produktem lub usługą. 67% klientów jest gotowych zapłacić więcej za towar, jeśli sposób obsługi będzie na najwyższym poziomie, a 67% ankietowanych w Ameryce Północnej uważa, że ich oczekiwania względem sprzedawcy są dziś większe niż kiedykolwiek.

Wynika z tego wprost, że dbając o wrażenia potencjalnego klienta, mamy większą szansę na sprzedaż – szybszą i za większą cenę. Dlatego już od pierwszego spotkania musimy być doskonale przygotowani, musimy mieć przy sobie wszystkie narzędzia sprzedażowe. Powinniśmy dysponować prezentacjami, multimediami, porównywarkami, konfiguratorami etc. Co więcej, metoda zapoznawania klienta z produktem musi być sprawdzona, ustrukturyzowana i sensowna, materiały muszą być atrakcyjne wizualnie, a oferty zrozumiałe dla każdego.

Brak danych

Zazwyczaj dyrektor sprzedaży, który korzysta tylko z danych z CRM, nie wie, ile dokładnie trwało spotkanie, jakie materiały zostały zaprezentowane, jakie informacje udało się zebrać sprzedawcy, co zainteresowało klienta i jaką konfigurację produktu mu przedstawiono. Nie ma narzędzia, które pozwoliłoby sprawdzić, czy klient otrzymał ofertę pocztą elektroniczną, czy przeczytał to, co mu wysłano, ile czasu poświęcił na zapoznanie się z ofertą i jakie jej elementy go zainteresowały.

Oczywiście, można wymusić na sprzedawcy robienie notatek zawierających takie informacje, ale sprzedawca ma sprzedawać, a nie tworzyć raporty do analizy. To oznacza, że musi się skupić na rozmowie i argumentacji, a nie na notowaniu. Proszę sobie wyobrazić, o ile wzrośnie czas potrzebny na obsługę CRM, jeśli nakaże się sprzedawcom robienie naprawdę szczegółowych notatek!

Już dziś w wielu raportach sprzedażowych możemy przeczytać, że sprzedawcy poświęcają zaledwie 36% swojego czasu na właściwą sprzedaż. Pozostały czas poświęcają na raportowanie i logistykę. To skrajnie nieefektywne. Co więc ma zrobić menedżer sprzedaży?

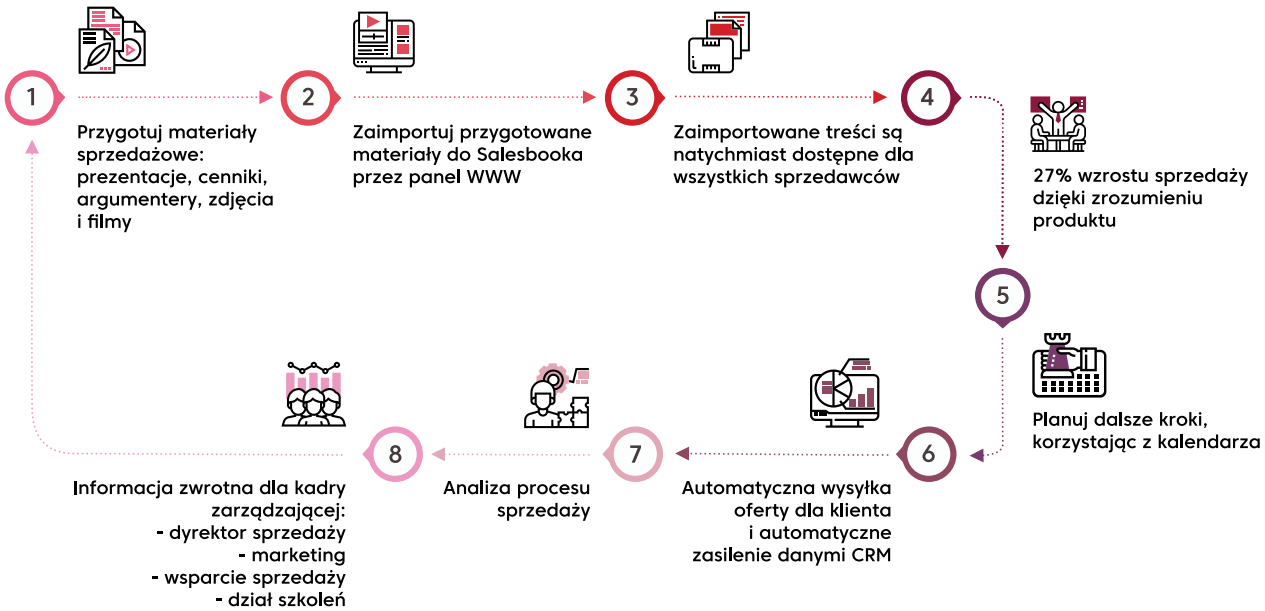
Narzędzia ułatwiające sprzedaż

W Polsce i na całym świecie są organizacje, które postanowiły ten stan rzeczy zmienić i sięgnęły po narzędzia mające ułatwić sprzedaż, przyśpieszyć ją (ang. *sales acceleration*). Zazwyczaj składają się one z dwóch głównych komponentów.

Pierwszy przeznaczony jest dla sprzedawcy. Otrzymuje on tablet z zainstalowaną aplikacją. Po jej uruchomieniu ma dostęp do wszystkich narzędzi marketingowo-sprzedażowych w formie elektronicznej: prezentacji, zdjęć, folderów, broszur technicznych, przykładów zastosowań etc. Ponieważ ma je w jednym miejscu, nie musi ich szukać. Może wybrać te materiały, które pomogą mu w danej rozmowie. Sprzedawca rozmawia z klientem, prezentuje produkt na tablecie, a kiedy spotkanie dobiegnie końca, narzędzie automatycznie przygotowuje ofertę i wysyła ją do wszystkich zainteresowanych.

Wyobraźmy sobie, że sprzedajemy usługi z dziedziny ochrony, które mają zapewnić bezpieczeństwo firmy lub domu. Nie jest to produkt łatwy do zaoferowania. Wymagana jest znajomość specjalistycznych terminów. Potrzebny jest też pewien zasób

Jak działa proces Sales Acceleration



Rys. 1. Narzędzia ułatwiające sprzedaż umożliwiają łatwe skonfigurowanie aplikacji dla doradców handlowych, a następnie skuteczną analizę menedżerską procesów sprzedażowych

informacji na temat klienta. Zamiast zmuszać go do żmudnego wypełniania ankiety, możemy użyć tabletu z kalkulatorem graficznym, dzięki któremu zbierzemy potrzebne informacje w kilka minut. Wykorzystamy przy tym symbole i obrazy, które lepiej przemawiają do wyobraźni niż zadawane pytania.

Drugi komponent jest przeznaczony dla menedżerów. Aplikacja automatycznie monitoruje wszystkie podjęte czynności – kiedy i gdzie zaczęło się spotkanie, ile trwało, jakie materiały zostały podczas niego wykorzystane, jaka oferta została złożona. Dzięki temu osoby zarządzające sprzedażą mogą dokonać analizy przebiegu procesu sprzedaży bezpośredniej. Na jej podstawie możliwa staje się kontrola czasu i jakości pracy doradców sprzedażowych. Można sprawdzić, jakie materiały wykorzystali. Widać też liczbę wysłanych ofert i umówionych spotkań.

Dostęp do tych danych mają nie tylko menedżerowie, ale także inni sprzedawcy. W ten sposób mogą podnosić swoje kwalifikacje – sprawdzanie, jak działają najlepsi, to bardzo skuteczna forma nauki.

Potwierdzenie w liczbach

Opracowany przez CSO Insights raport pt. *Sales Enablement Report* informuje, że sprzedawcy, którzy są wspomagani przez aplikacje ułatwiające sprzedaż, sprzedają więcej niż ich koledzy, którzy posługują się bardziej tradycyjnymi narzędziami. W roku 2018 odsetek przedstawicieli, którzy zrealizowali założenia budżetowe, wzrósł aż o 10,6 punktu procentowego (do poziomu 43%), co stanowi poprawę aż o 22,7%.

Stwierdzenie, że klienci nie lubią lub nie chcą spotkań z handlowcami, okazuje się nieprawdziwe – chcą, tylko pod pewnymi warunkami. Najważniejsze jest to, by takie spotkanie miało wartość poznawczą. Sposób prezentacji oferty powinien wskazywać na możliwość rozwiązania konkretnych problemów potencjalnego nabywcy.

W przygotowanym przez CSO Insights raporcie pt. *The Growing Buyer-Seller Gap* znajdziemy ciekawe informacje na ten temat. Otóż, aż 65,2% badanych, którzy spotykali się z przedstawicielami korzystającymi z narzędzi ułatwiających sprzedaż, uznało takie spotkanie za wartościowe; 61,8% orzekło, że spotkanie spełniło ich oczekiwania, a 32,2% stwierdziło, że oferta i sposób prezentacji przekroczyły ich oczekiwania. Tylko 2,6% ankietowanych chciało zrobić zakup on-line, bez wsparcia ze strony sprzedawcy.

Światło w tunelu

Branża usług ochrony może zrewolucjonizować sposób dystrybucji swoich produktów, jeśli połączy tradycję z nowoczesnością. Szansą dla niej są rozwiązania ułatwiające sprzedaż, które sytuują sprzedawcę w centrum uwagi i wykorzystują zdobycze współczesnej techniki (tablet, analizę w czasie rzeczywistym i uczenie maszynowe), by wyposażyć go w broń, której jeszcze nikt wcześniej nie miał.

Dariusz Nawojczyk
salesbook-app.com
dariusz.nawojczyk@salesbook-app.com

AST DO BRAM DRZWI OKIEN

2 GRADE

CZUJKI MAGNETYCZNE DO BRAM, DRZWI i OKIEN

TERAZ ZE STOPNIEM ZABEZPIECZENIA GRADE 2

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

AAT HOLDING S.A.
ul. Puławska 431
02-801 Warszawa
tel. 22 546 05 46; faks 22 546 05 01
e-mail: kontakt@aat.pl
www.aat.pl

D PROD S

Oddziały:
ul. Koniczynowa 2A, 03-612 Warszawa II
tel./faks 22 743 10 11, 811 13 50
e-mail: aat.warszawa-praga@aat.pl

ul. Antoniuk Fabryczny 22, 15-741 Białystok
tel. 85 688 32 33
tel./faks 85 688 32 34
e-mail: aat.bialystok@aat.pl

ul. Łęczycka 37, 85-737 Bydgoszcz
tel./faks 52 342 91 24, 342 98 82
e-mail: aat.bydgoszcz@aat.pl

ul. Ks. W. Siwka 17, 40-318 Katowice
tel./faks 32 351 48 30, 256 60 34
e-mail: aat.katowice@aat.pl

ul. Prosta 25, 25-371 Kielce
tel./faks 41 361 16 32, 361 16 33
e-mail: aat.kielce@aat.pl

ul. Biskupińska 14, 30-732 Kraków
tel./faks 12 266 87 95, 266 87 97
e-mail: aat.krakow@aat.pl

ul. Dowborczyków 25, 90-019 Łódź
tel./faks 42 674 25 33, 674 25 48
e-mail: aat.lodz@aat.pl

ul. Racławicka 82, 60-302 Poznań
tel./faks 61 662 06 60, 662 06 61
e-mail: aat.poznan@aat.pl

Al. Niepodległości 606/610, 81-855 Sopot
tel./faks 58 551 22 63, 551 67 52
e-mail: aat.sopot@aat.pl

ul. Zielona 42, 71-013 Szczecin
tel./faks 91 483 38 59, 489 47 24
e-mail: aat.szczecin@aat.pl

ul. Na Niskich Łąkach 26, 50-422 Wrocław
tel./faks 71 348 20 61, 348 42 36
e-mail: aat.wroclaw@aat.pl

ACSS ID Systems Sp. z o.o.
ul. Karola Miarki 20C
01-496 Warszawa
tel. 22 832 47 44; faks 22 832 46 44
e-mail: biuro@acss.com.pl
www.acss.com.pl

D I PROJ S

ALARMNET BORKIEWICZ Sp. J.
ul. Karola Miarki 20c
01-496 Warszawa
tel. 22 663 40 85
e-mail: biuro@alarmnet.com.pl
www.alarmnet.com.pl

D PROJ S

ALARMTECH POLSKA Sp. z o.o.
Oddział w Gdańsku
ul. Kielnieńska 115
80-299 Gdańsk
tel. 58 340 24 40; faks 58 340 24 49
e-mail: info@alarmtech.pl
www.alarmtech.pl

D PROD PROJ S

ALARM-TECH Systemy Zabezpieczeń s.c.
ul. Graniczna 4
32-086 Boleń
tel. kom. 775 453 453
e-mail: sklep@napad.pl
www.napad.pl

Oddział:
os. Jagiellońskie 19, 31-834 Kraków
tel. kom. 609 197 800

D PROD S

ASSA ABLOY POLAND Sp. z o.o.
ul. Iłżecka 24 bud. F
02-135 Warszawa
tel. 22 751 53 54; faks 22 751 53 56
e-mail: biuro@assaabloy.com
www.assaabloy.com.pl

D I PROD PROJ S

ROBERT BOSCH Sp. z o.o.
ul. Jutrzenki 105
02-231 Warszawa
tel. 22 715 00 00
e-mail: securitysystems@pl.bosch.pl
www.boschsecurity.pl

C D PROJ S

P.W.H. BRABORK LABORATORIUM Sp. z o.o.
ul. Ratuszowa 11
03-450 Warszawa
tel. 22 619 29 49, 619 25 14
faks 22 619 25 14
e-mail: brabork@braborklab.pl
www.braborklab.pl

I PROJ

BT Electronics Sp. z o.o.
ul. Rybitwy 22
30-722 Kraków
tel. 12 410 20 33, faks 12 410 85 11
e-mail: bte@bte.pl
www.bte.pl

D I PROD PROJ S

CBC (Poland) Sp. z o.o.
ul. Anny German 15
01-794 Warszawa
tel. 22 633 90 90
e-mail: info@cbcpoland.pl
www.cbcpoland.pl

D PROD S

CONTROL SYSTEM FMN
Al. KEN 96 lok. U-15
02-777 Warszawa
tel. 22 855 00 17
e-mail: cs@cs.pl
www.cs.pl

D I PROD PROJ S

DAHUA TECHNOLOGY POLAND Sp. z o.o.
ul. Salsy 2
02-823 Warszawa
tel. 22 395 74 00
e-mail: biuro.pl@dahuatech.com
www.dahuasecurity.com/pl

DG ELPRO Sp. J.
ul. Bonarka 21
30-415 Kraków
tel. 12 263 93 85; faks 12 263 93 86
email: biuro@dgelpro.pl
www.dgelpro.pl

DYSKRET POLSKA
Spółka z ograniczoną odpowiedzialnością Sp. K.
ul. Mazowiecka 131
30-023 Kraków
tel. 12 423 31 00; faks 12 423 44 61
e-mail: office@dyskret.com
www.dyskret.com

EBS Sp. z o.o.
ul. Bronisława Czecha 59
04-555 Warszawa
tel. 22 518 84 00
e-mail: office@ebs.pl
www.ebssmart.com

ELTROX
ul. Główna 23
42-280 Częstochowa
tel. 34 333 57 04
e-mail: sklep@eltrox.pl
www.eltrox.pl

Oddziały:
ul. Św. Rocha 87, 42-202 Częstochowa
tel. 34 333 57 13
e-mail: czestochowa@eltrox.pl

ul. Hynka 6/2, 80-465 Gdańsk
tel. kom. 517 015 441
e-mail: gdansk@eltrox.pl

ul. Myśliborska 2-6, 66-400 Gorzów Wlkp.
tel. 95 766 65 16
e-mail: gorzow@eltrox.pl

ul. Wybickiego 42a, 31-302 Kraków
tel. 12 210 06 25
e-mail: krakow@eltrox.pl

ul. 6 sierpnia 14, 90-416 Łódź
tel. 42 233 49 96
e-mail: lodz@eltrox.pl

ul. Orla 7/I, 41-205 Sosnowiec
tel. kom. 501 945 219
e-mail: sosnowiec@eltrox.pl

ul. ks. kard. S. Wyszyńskiego 22
70-203 Szczecin
tel. 91 443 56 36
e-mail: szczecin@eltrox.pl

ul. Joachima Lelewela 33, 87-100 Toruń
tel. 56 645 94 24
e-mail: torun@eltrox.pl

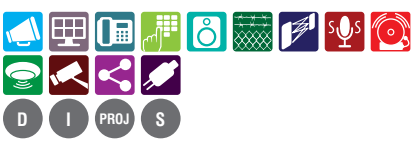
ul. Radzymińska 308, 03-694 Warszawa
tel. 22 676 78 40
e-mail: warszawa@eltrox.pl

ul. Komandorska 53R, 50-258 Wrocław
tel. kom. 504 904 689
e-mail: wroclaw@eltrox.pl

ES-INSTAL Andrzej Wójcik
Al. gen. W. Sikorskiego 9 A/72 A
02-758 Warszawa
tel. kom. +48 501 277 513
e-mail: andrzejw@esinstal.pl
https://esinstal.pl/

EWIMAR Sp. z o.o.
ul. Konarskiego 84
01-355 Warszawa
tel. 22 691 90 65
e-mail: handel@ewimar.pl
www.ewimar.pl

FES TRADING Sp. z o.o.
ul. Schuberta 100
80-171 Gdańsk
tel. 58 340 00 41 ÷ 44; faks 58 340 00 45
e-mail: fes@fes.pl
www.fes.pl



GDE POLSKA
Leszek Mitusiński
Włosań, ul. Świątnicka 88
32-031 Mogilany
tel. 12 256 50 25, 12 256 50 35;
faks 12 270 56 96
e-mail: biuro@gde.pl
www.gde.pl

ICS POLSKA
ul. Poleczki 82
02-822 Warszawa
tel. 22 646 11 38; faks 22 849 94 83
e-mail: biuro@ics.pl
www.ics.pl

INSAP Sp. z o.o.
ul. Ładna 4-6
31-444 Kraków
tel. 12 411 49 79, 411 57 47; faks 12 411 94 74
e-mail: insap@insap.pl
www.insap.pl

JANEX INTERNATIONAL Sp. z o.o.
ul. Płomyka 2
02-490 Warszawa
tel. 22 863 63 53; faks 22 863 74 23
e-mail: sekretariat@janexint.com.pl
www.janexint.com.pl

KOLEKTOR
K. MIKICIUK I R. RUTKOWSKI Sp. J.
ul. Obrońców Westerplatte 31
80-317 Gdańsk
tel. 58 553 67 59; faks 58 553 48 67
e-mail: info@kolektor.pl
www.kolektor.pl

MICROMADE
Gałka i Drożdż Sp. J.
ul. Wieniawskiego 16
64-920 Piła
tel./faks 67 213 24 14
e-mail: mm@micromade.pl
https://micromade.pl/

MICRONIX Sp. z o.o.
ul. Spółdzielcza 10
58-500 Jelenia Góra
tel. 75 755 78 78
e-mail: info@micronix.pl
www.micronix.pl

POLON-ALFA S.A.
ul. Glinki 155
85-861 Bydgoszcz
tel. 52 363 92 61; faks 52 363 92 64
e-mail: polonalfa@polon-alfa.pl
www.polon-alfa.pl

PROFICCTV Sp. z o.o.
ul. Strzeszyńska 66
60-479 Poznań
tel./faks 61 842 29 62
e-mail: biuro@profisystems.pl
www.profisystems.pl

RETT-POL
Bogusław Godlewski
ul. Podmiejska 21
01-498 Warszawa
tel. 22 632 72 22; faks 22 833 09 07
e-mail: biuro@rettpol.pl
www.rettpol.pl

Oddział:
ul. Sportowa 3, 35-111 Rzeszów
tel. 17 785 18 16; faks 22 833 09 07
e-mail: rzeszow@rettpol.pl

ROPAM Elektronik s.c.
Polanka 301
32-400 Myślenice
tel. 12 272 39 71, 341 04 07; faks 12 379 34 10
www.ropam.com.pl

ROGER Sp. z o.o. Sp. k.
Gościszewo 59
82-400 Sztum
tel. 55 272 01 32
faks 55 272 01 33
e-mail: roger@roger.pl
www.roger.pl

SCHRACK SECONET POLSKA Sp. z o. o.
Wilanów Office Park, bud. B1
ul. Adama Branickiego 15
02-972 Warszawa
tel./faks 22 33 00 620/624
e-mail: warszawa@schrack-seconet.pl
www.schrack-seconet.pl

Oddziały:
ul. M. Gomółki 2, 80-279 Gdańsk
tel. 58 526 35 70
e-mail: gdansk@schrack-seconet.pl

ul. Jasnogórska 23 lok. 17
(wejście od ul. Stawowej)
31-358 Kraków
tel. 12 637 11 74
e-mail: krakow@schrack-seconet.pl

ul. Św. Czesława 7 lok. 18, 61-575 Poznań
tel./faks 61 833 31 53, 833 50 37
e-mail: poznan@schrack-seconet.pl

ul. Mydlana 1, 51-502 Wrocław
tel./faks 71 345 00 95
e-mail: wroclaw@schrack-seconet.pl

smart-technologie
SYSTEMY OGNIOCHRONNE
TECHNIKA MONTAŻU BEZPOŚREDNIEGO

SMART-EKO Jarosław Szkaradek
(SMART-TECHNOLOGIE.PL)
ul. Domagały 1
30-741 Kraków
tel. kom. +48 791 061 485, 793 061 485
e-mail: biuro@smart-eko.pl
www.smart-technologie.pl

TAP - Systemy Alarmowe Sp. z o.o.
ul. Tatrzańska 8
60-413 Poznań
tel./faks 61 677 48 00
e-mail: tap@tap.com.pl
www.tap.com.pl

TECHOM

Zakład Rozwoju Technicznej Ochrony Mienia
TECHOM Sp. z o.o.
Al. Wyzwolenia 12
00-570 Warszawa
tel. 22 625 34 00
e-mail: techom@techom.com
www.techom.com

W2 Włodzimierz Wyrzykowski
ul. Ceramiczna 1A
86-005 Kruszyn Krajeński
tel. 52 522 32 38
e-mail: biuro@w2.com.pl
www.w2.com.pl

Always precise WINKHAUS

WINKHAUS POLSKA BETEILIGUNGS
Spółka z ograniczoną odpowiedzialnością Sp.K.
ul. Przemysłowa 1
64-130 Rydzyna
tel. 65 525 57 00
faks 65 525 58 00
e-mail: winkhaus@winkhaus.pl
www.winkhaus.pl

Legenda

Kategorie*

- bezpieczeństwo IT
- biometria
- DSO
- monitoring
- ochrona fizyczna
- RFID
- systemy domofonowe i wideodomofonowe
- systemy komunikacyjne
- systemy kontroli dostępu
- systemy nagłośnieniowe
- systemy ochrony peryferyjnej
- systemy ochrony zewnętrznej
- systemy przeciwkradzieżowe
- systemy przywoławcze
- systemy sygnalizacji pożarowej
- systemy sygnalizacji włamania i napadu
- systemy telewizji dozorowej
- systemy zintegrowane
- zabezpieczenia mechaniczne
- zasilanie

Działalność*

- B badania
- C certyfikacja
- D dystrybucja
- I instalacja
- PROJ projektowanie
- PROD produkcja
- S szkolenia

* Szybkie wyszukiwanie przez filtrowanie na naszej stronie www.zabezpieczenia.com.pl

ZABEZPIECZENIA

dwumiesięcznik

Redaktor naczelny
Teresa Karczmarzyk

Redaktorzy merytoryczni
Stanisław Banaszewski
Paweł Karczmarzyk
Andrzej Walczyk

Korekta
Paweł Karczmarzyk

Dział marketingu i reklamy
Ela Końka

Redaguje zespół
Marek Blim
Patryk Gańko
Norbert Góra
Daniel Kamiński
Paweł Karczmarzyk
Arkadiusz Milka
Adam Rosiński
Ryszard Sobierski
Waldemar Szulc
Andrzej Wójcik

Współpraca
Marcin Buczaj
Piotr Czernoch
Marcin Pyclik

Projekt graficzny, skład i łamanie
Piotr Przybylski

Adres redakcji
ul. Przy Bażantarni 13
02-793 Warszawa
tel. 22 670 09 19
faks 22 649 97 19
www.zabezpieczenia.com.pl

Wydawca
AAT HOLDING S.A.
ul. Puławska 431, 02-801 Warszawa
tel. 22 546 0 546
faks 22 546 0 501

Druk
Regis Sp. z o.o.
ul. Napoleona 4, 05-230 Kobyłka

Dostępne formy reklamy

Reklama wewnątrz czasopisma
cała strona, pełny kolor
cała strona, czarno-biała
1/2 strony, pełny kolor
1/2 strony, czarno-biała
1/3 strony, pełny kolor
1/3 strony, czarno-biała
1/4 strony, pełny kolor
1/4 strony, czarno-biała
karta katalogowa, 1 strona

Reklama na okładkach
pierwsza strona
druga strona
przedostatnia strona
ostatnia strona

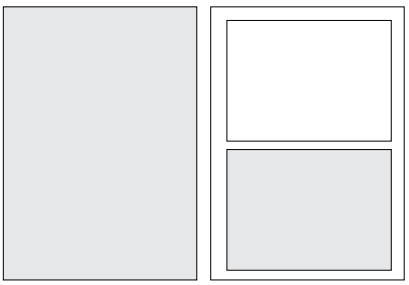
Artykuł sponsorowany
Forma graficzna artykułu sponsorowanego podlega zasadom jednolitym dla wszystkich materiałów zamieszczonych w czasopiśmie

Spis teleadresowy
Redakcja przyjmuje zamówienia na 6 kolejnych emisji

Ceny negocjujemy indywidualnie

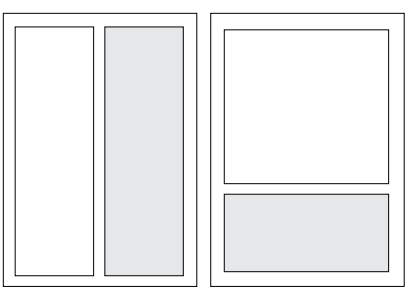
Warunki techniczne przyjmowanych reklam dostępne są na stronie internetowej http://www.zabezpieczenia.com.pl w dziale Reklama

Udostępniamy również powierzchnię reklamową na naszej stronie internetowej http://www.zabezpieczenia.com.pl



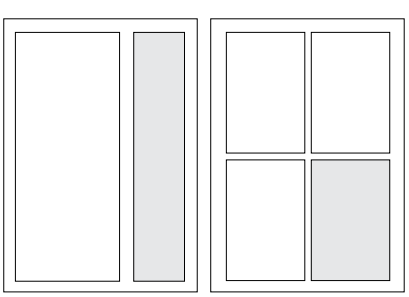
cała strona
(200 x 282 mm + 3mm spad)

1/2 strony
(170 x 125 mm)



1/2 strony
(83 x 260 mm)

1/3 strony
(170 x 80 mm)



1/3 strony
(54 x 260 mm)

1/4 strony
(83 x 125 mm)

Spis reklam

NMS ACCESS CONTROL

PROFESJONALNE ROZWIĄZANIE
DO SYSTEMÓW KONTROLI DOSTĘPU
I NADZORU WIZYJNEGO

POZNAJ
NAJNOWSZE OPROGRAMOWANIE

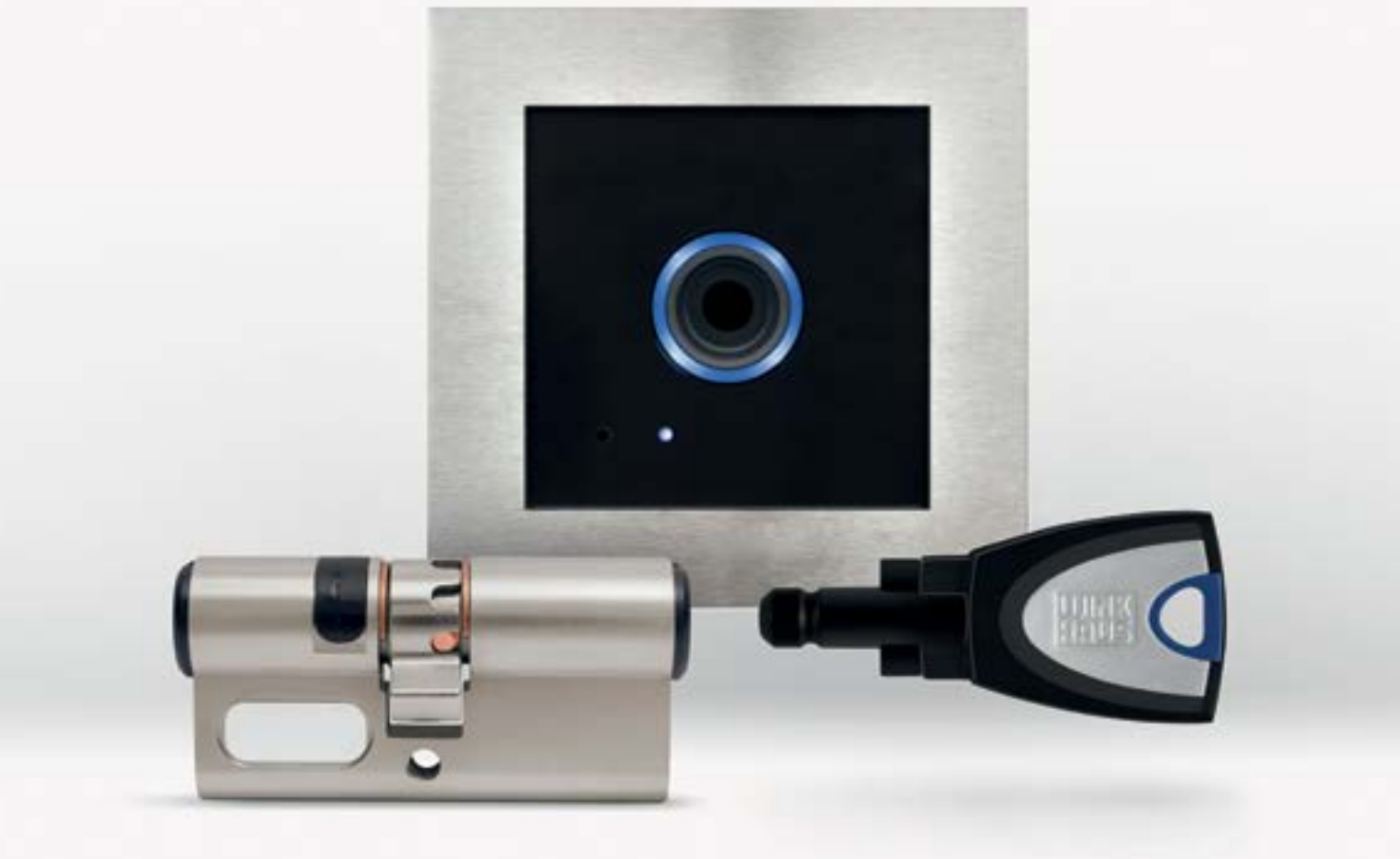
ODWIEDŹ NASZ ODDZIAŁ
JUŻ DZIŚ!

www.nmsac.aat.pl

Wielostanowiskowa obsługa systemu, struktura typu SERWER – KLIENT
Współpraca z nowymi kontrolerami serii KS3000
Bezpieczna baza typu MS SQL dla danych i zdarzeń
Integracja z rejestratorami NVR i kamerami IP marki NOVUS

AAT HOLDING S.A.
PRODUCENT I DOSTAWCA ELEKTRONICZNYCH SYSTEMÓW ZABEZPIECZENIA MIENIA
www.aat.pl

Always precise



Elektroniczne systemy dostępowe Winkhaus

Łatwość instalacji na każdym etapie inwestycji

Winkhaus blueSmart to system elektronicznych wkładek z własnym zasilaniem oraz elektronicznych kluczy, który pozwala efektywnie zarządzać prawami dostępu w budynku. Za pomocą centralnego czytnika klucze komunikują się z oprogramowaniem, tworząc sieć wirtualną. Ze względu na brak okablowania funkcjonujący w ten sposób system jest łatwy w montażu oraz niezwykle elastyczny i tani w eksploatacji.

- Błyskawiczna, bezkosztowa zmiana dostępu
- Wysoki poziom bezpieczeństwa (IMP klasa 6.2)
- Brak okablowania
- Łatwy i szybki montaż
- Dyskretna stylistyka